(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－3129
（P2000－3129A）
(43)公開日　平成12年１月７日(2000.1.7)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｃ０７６
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		

審査請求　有　　請求項の数15　ＯＬ　（全 27 頁）

(21)出願番号　特願平10－122108

(22)出願日　平成10年５月１日(1998.5.1)

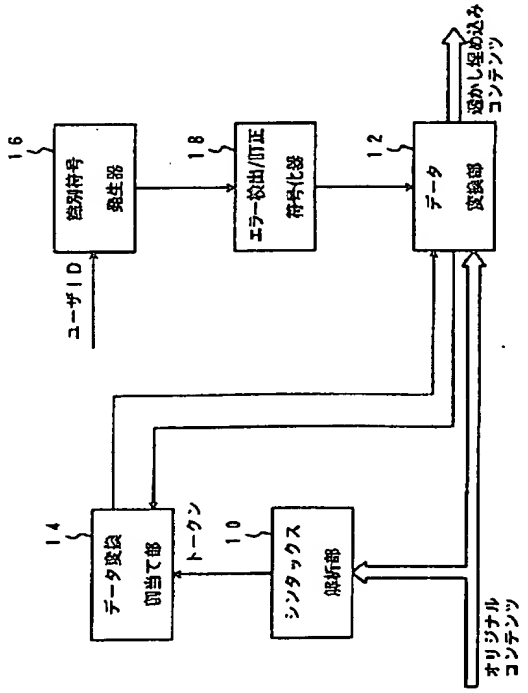
(31)優先権主張番号　特願平10－108039
(32)優先日　平成10年４月17日(1998.4.17)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　396001360
株式会社ディジタル・ビジョン・ラボラトリーズ
東京都港区赤坂七丁目３番37号
(72)発明者　村谷　博文
東京都港区赤坂七丁目３番37号　株式会社ディジタル・ビジョン・ラボラトリーズ内
(74)代理人　100058479
弁理士　鈴江　武彦　（外５名）

Ｆターム(参考)　5B017 AA06 BA05 BA07 BB10 CA16
5C076 AA14 AA40 BA06

(54)【発明の名称】　電子透かし埋め込み装置

(57)【要約】
【課題】複数のユーザが結託して互いのデータを比較したとしても、透かしデータを改竄することが困難であるような透かしデータを埋め込む電子透かし埋め込み装置を提供することである。
【解決手段】ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を埋め込むことにより、たとえ複数のユーザが結託して、差分データを改竄して、自分達のデータ以外のデータに書換えたと思っても、改竄後のデータに自分達を示すデータが残ってしまい、結託が失敗する。



【特許請求の範囲】

【請求項１】　ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、
ユーザを識別する情報として、ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする電子透かし埋め込み装置。

【請求項２】　ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、
ユーザを識別する情報として、当該ユーザがディジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を用いることを特徴とする電子透かし埋め込み装置。

【請求項３】　ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、
ユーザを識別する情報として、ディジタルデータを渡す可能性のあるユーザのの各々に順位を付け、当該ユーザが各ユーザより順位が小さいか、等しいか、あるいは大きいかを表わす情報を用いることを特徴とする電子透かし埋め込み装置。

【請求項４】　ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、
ユーザを識別する情報として、ディジタルデータを渡す可能性のあるユーザのの各々に順位を付け、ディジタルデータを渡す可能性のあるユーザの総数をＮとし、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑそれぞれに対して、ｐを法とした当該ユーザの順位ｎの剰余が０からｐ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報と、ｑを法とした当該ユーザの順位ｎの剰余が０からｑ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報とをユーザを識別する情報として用いることを特徴とする電子透かし埋め込み装置。

【請求項５】　ユーザに渡すディジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、
対象を識別する情報として、全識別対象の中の任意の２つの識別対象の各々に対して、識別すべき対象がその対に含まれているか否かを表わす情報を発生することを特徴とする識別情報発生装置。

【請求項６】　ユーザに渡すディジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、
対象を識別する情報として、識別すべき対象が全識別対象の各々であるか否かを表わす情報を発生することを特徴とする識別情報発生装置。

【請求項７】　ユーザに渡すディジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、
対象を識別する情報として、全識別対象の各々に順位を付け、識別すべき対象が各識別対象より順位が小さいか、等しいか、あるいは大きいかを表わす情報を発生することを特徴とする識別情報発生装置。

【請求項８】　ディジタルデータを渡す可能性のあるユーザの総数をＮとし、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑそれぞれに対して、ｐを法とした当該ユーザの順位ｎの剰余が０からｐ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報と、ｑを法とした当該ユーザの順位ｎの剰余が０からｑ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報とをユーザを識別する情報として用いることを特徴とする請求項７に記載の識別情報発生装置。

【請求項９】　ディジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、
種々のデータ変換内容を記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、
識別対象固有の情報に応じて、識別符号を発生する手段と、
前記データ割当て部から出力されたデータ変換内容と前記識別符号に応じて、ディジタルデータの所定の部分を変更する識別符号埋め込み手段と、
を具備することを特徴とする識別符号埋め込み装置。

【請求項１０】　ディジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、
種々のデータ変換内容をその変化程度を表わすコストと共に記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、
データ変換後のデータの変化程度を累積する手段と、
識別対象固有の情報に応じて、識別符号を発生する手段と、
前記データ割当て部から出力されたデータ変換内容と前記識別符号に応じて、ディジタルデータの所定の部分を変更する識別符号埋め込み手段と、
前記累積手段により、データの変化程度の累積値が所定の変化程度を超える場合、前記識別符号埋め込み手段の動作を禁止する手段とを具備することを特徴とする識別符号埋め込み装置。

【請求項１１】　識別情報がユーザには知覚できないように埋め込まれているディジタルデータから識別情報を読み取る識別情報検出装置において、

ディジタルデータの所定の位置に埋め込まれている識別符号を抽出する手段と、
抽出された識別符号を復号し、識別情報を求める手段と、
を具備することを特徴とする識別情報検出装置。
【請求項１２】　請求項１に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、
ディジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、
その部位が請求項１に記載の装置により埋め込まれた、そのユーザ対がこのディジタルデータに対応するユーザを含んでいることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、
その部位が請求項１に記載の装置により埋め込まれた、そのユーザ対がこのディジタルデータに対応するユーザを含んでいることを表わす符号であると判定されたユーザ対を結託したユーザ対の候補と推定することを特徴とする識別情報読取方法。
【請求項１３】　請求項２に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、
ディジタルデータから抽出された識別情報から各ユーザに対応する部位を読み取るステップと、
その部位が請求項２に記載の装置により埋め込まれた、そのユーザがこのディジタルデータに対応するユーザであることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、
その部位が請求項２に記載の装置により埋め込まれた、そのユーザがこのディジタルデータに対応するユーザであることを表わす符号であると判定されたユーザを結託したユーザの候補と推定することを特徴とする識別情報読取方法。
【請求項１４】　請求項３に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、
１）ディジタルデータから抽出された識別情報から各ユーザに対応する部位を順次読み取るステップと、
２）その部位が請求項３に記載の装置により埋め込まれた、そのユーザの順位がこのディジタルデータに対応するユーザの順位よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ１）、２）を繰り返すステップと、
３）上記ステップ２）において、初めて現れたそれ以外の符号の次の部位から、各ユーザに対応する部位を順次読み取るステップと、
４）その部位が請求項３に記載の装置により埋め込まれた、そのユーザの順位がこのディジタルデータに対応するユーザの順位よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ３）、４）を繰り返すステップと、
５）抽出された識別情報の最後に到達するまで上記ステップ３）、４）、５）を繰り返すステップと、を具備し、
上記ステップ２）において、それ以外の符号が初めて現れた部位に対応するユーザを第一の結託ユーザ候補と推定し、
上記ステップ４）において、それ以外の符号が最後に現れた部位に対応するユーザを第二の結託ユーザ候補と推定することを特徴とする識別情報読取方法。
【請求項１５】　請求項４に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、
１）ディジタルデータから抽出された識別情報からｐを法とするユーザのそれぞれに対応する部位を順次読み取るステップと、
２）その部位が、請求項４に記載の装置により埋め込まれた、ｐを法としたそのユーザの順位の剰余がｐを法としたこのディジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ１）、２）を繰り返すステップと、
３）上記ステップ２）において、初めて現れたそれ以外の符号を次の部位から、ｐを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
４）その部位が、請求項４に記載の装置により埋め込まれた、ｐを法としたそのユーザ順位の剰余がｐを法としたこのディジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ３）、４）を繰り返すステップと、
５）抽出された識別情報からｐを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ３）、４）、５）を繰り返すステップと、
６）上記ステップ５）において、抽出された識別情報からｐを法としたユーザ順位の剰余のすべての部位を読み取った後、その次の部位からｑを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
７）その部位が、請求項４に記載の装置により埋め込まれた、ｑを法としたそのユーザの順位の剰余がｑを法としたこのディジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ６）、７）を繰り返すステップと、
８）上記ステップ７）において、初めて現れたそれ以外の符号を次の部位から、ｑを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

９）その部位が、請求項４に記載の装置により埋め込まれた、ｑを法としたそのユーザ順位の剰余がｑを法としたこのディジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ８）、９）を繰り返すステップと、
１０）抽出された識別情報からｑを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ８）、９）、１０）を繰り返すステップと、を具備し、
上記ステップ２）において、それ以外の符号が初めて現れた部位に対応するｐを法としたユーザ順位の剰余と、
上記ステップ４）において、それ以外の符号が最後に現れた部位に対応するｐを法としたユーザ順位の剰余と、
上記ステップ７）において、それ以外の符号が初めて現れた部位に対応するｑを法としたユーザ順位の剰余と、
上記ステップ９）において、それ以外の符号が最後に現れた部位に対応するｑを法としたユーザ順位の剰余とを組み合わせて構成されるｐを法とする剰余とｑを法とする剰余の組に対して中国人剰余定理を適用して結託ユーザの候補を推定することを特徴とする識別情報読取方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は音声や画像等のディジタル著作物データに、そのデータの著作権者、ユーザ等に関するなんらかの情報（以下、透かしデータと称する）を著作権者、ユーザ等には知覚できない状態で埋め込み、隠し持たせる電子透かし埋め込み装置に関する。

【０００２】

【従来の技術】ディジタル技術の進歩により、映画、音楽、写真等の様々な著作物がディジタルデータ（ディジタル著作物）として流通されている。そのため、ディジタル著作物の著作権を巡る問題が深刻になってきている。近年、ディジタル著作物の不正利用を防止するための技術として電子透かし技術が脚光を浴びてきている。この技術は、データの著作権者、提供者等の権利を保護するために、データの中に著作権者、提供者、ユーザに関する情報等を、ユーザには判別できない形で埋め込みし、不正利用があった場合に、そのユーザを特定できるようにするものである。この情報は電子透かし、ウォーターマーク、フィンガープリントと呼ばれる。

【０００３】不正利用の防止についてさらに詳細に説明すると、著作権者はディジタル著作物を流通させる際に、ユーザを識別する透かしデータを埋め込んでおく。ユーザが著作権者の許可無く、ディジタル著作物を無断で複製し、第３者に販売等を行うことがある。著作権者は不正と思われるコピーを発見したら、そのデータから透かしデータを検出し、無断複製、不正販売を行ったユーザを特定し、そのユーザにペナルティを課すことができる。透かしデータの種類や、ディジタルデータへの埋め込み箇所はユーザには分からないようになっているので、ユーザは透かしデータを取り除くことはできない。

【０００４】しかし、透かしデータはユーザを識別する情報であり、ユーザ毎に異なるので、２人以上のユーザが結託すると、透かしデータの存在が簡単に分かってしまう欠点がある。すなわち、ユーザＡとユーザＢが互いのデータの差分をとると、ユーザＡの透かしデータとユーザＢの透かしデータそのものは識別できないものの、その埋め込み箇所は想定できる。そのため、ユーザはこれらの差分データに何らかの信号を加えることにより、透かしデータを改竄することができる。

【０００５】例えば、ディジタルデータがＭＰＥＧ方式の動画像である場合、３人のユーザをユーザＡ、Ｂ、Ｃとし、２ビットのディジタルデータで３人のユーザの識別のための透かし情報を埋め込む。ユーザＡの識別符号を“１０”、ユーザＢの識別符号を“０１”、ユーザＣの識別符号を“１１”とする。識別符号“００”はどのユーザも識別しない。これらの２ビットの識別符号の埋め込み方は、１ビット目はｉ番目のフレームの（ｘ、ｙ）画素の輝度データに埋め込み、その１ビット目のデータが“１”の場合は輝度データＶをＶ＋１とし、“０”の場合は輝度データＶをＶのままとし、２ビット目はｊ番目のフレームの（ｖ、ｗ）画素の輝度データに埋め込み、その２ビット目のデータが“１”の場合は輝度データＶ’をＶ’＋１とし、“０”の場合は輝度データＶ’をＶ’のままとすることにより、埋め込む。

【０００６】そのため、ｉ番目のフレームの（ｘ，ｙ）画素、ｊ番目のフレームの（ｖ，ｗ）画素の輝度データを調べるとユーザを特定できる。ユーザＡの識別符号“１０”は（Ｖ＋１，Ｖ’）、ユーザＢの識別符号“０１”は（Ｖ，Ｖ’＋１）である。

【０００７】ユーザＡ、Ｂは互いのデータを比較して、ｉ番目のフレームの（ｘ，ｙ）画素、ｊ番目のフレームの（ｖ，ｗ）画素の輝度データが違うことが分かり、これらの輝度データにユーザを識別する透かしデータが埋め込まれていることが分かる。そして、これらの輝度データを書換えて、自分達を示す情報以外の識別情報に改竄したい。

【０００８】
（ｉ；ｘ，ｙ）：（Ｖ＋１、またはＶ）→Ｖ＋ΔＶ
これは、ｉ番目のフレームの（ｘ，ｙ）画素の輝度データＶ＋１、またはＶをＶ＋ΔＶに書換えることを示す。

【０００９】（ｊ；ｖ，ｗ）：（Ｖ’、またはＶ’＋１）→Ｖ’＋ΔＶ’
これは、ｊ番目のフレームの（ｖ，ｗ）画素の輝度データＶ’、またはＶ’＋１をＶ’＋ΔＶ’に書換えることを示す。

【００１０】ΔＶ、ΔＶ’をどのように選ぶかを考える。

【００１１】（イ）ΔＶ＝１、ΔＶ’＝０これは、ユー

ザＡの識別符号と同じである。
【００１２】（ロ）ΔＶ＝０、ΔＶ’＝１
これは、ユーザＢの識別符号と同じである。
【００１３】（ハ）ΔＶ＝１、ΔＶ’＝１
これは、ユーザＣの識別符号である。
【００１４】（ニ）ΔＶ＝０、ΔＶ’＝０
この識別符号が定義されておらず、誰も特定しない。
【００１５】このため、ユーザＡ、Ｂは（イ）、（ロ）の場合は自分達を示す識別情報に書き換わってしまい、ΔＶ、ΔＶ’をこれ以外のデータに書き換えればよいことが分かる。もちろん、ユーザＡ、Ｂは（ハ）、（ニ）の書換え後の識別情報が具体的には何を意味しているかを認識してはいないが、これらのように書換えると、自分達を示す識別情報を改竄できることが想像できる。
【００１６】以上に述べた透かしデータの埋め込みは一例であって、透かしデータはディジタルデータに対するより一般的な変換操作として多様な埋め込みが可能である。
【００１７】
【発明が解決しようとする課題】このように従来の電子透かし埋め込み技術は、ユーザを識別する透かしデータを当該ユーザには知覚できない状態で埋め込み、隠し持たせることができるが、複数のユーザが結託してデータを互いに比較することにより、透かしデータが埋め込まれている位置に関する情報を得ることができてしまい、透かしデータの偽造や消去を容易にするという欠点があった。
【００１８】本発明の目的は、複数のユーザが結託して互いのデータを比較したとしても、埋め込まれている透かしデータに関する情報を十分に得ることができず、透かしデータを偽造や消去することが困難となるように、ディジタルデータに、そのデータのユーザ等に関する透かしデータを埋め込み、隠し持たせる電子透かし埋め込み装置を提供することである。
【００１９】
【課題を解決するための手段】上記課題を解決し目的を達成するために、本発明は以下に示す手段を用いている。
【００２０】（１）ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする。
【００２１】（２）ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、当該ユーザがディジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を用いることを特徴とする。
【００２２】（３）ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、ディジタルデータを渡す可能性のあるユーザのの各々に順位を付け、当該ユーザが各ユーザより順位が小さいか、等しいか、あるいは大きいかを表わす情報を用いることを特徴とする。
【００２３】（４）ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、ディジタルデータを渡す可能性のあるユーザのの各々に順位を付け、ディジタルデータを渡す可能性のあるユーザの総数をＮとし、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑそれぞれに対して、ｐを法とした当該ユーザの順位ｎの剰余が０からｐ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報と、ｑを法とした当該ユーザの順位ｎの剰余が０からｑ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報とをユーザを識別する情報として用いることを特徴とする。
【００２４】（５）ユーザに渡すディジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、対象を識別する情報として、全識別対象の中の任意の２つの識別対象の各々に対して、識別すべき対象がその対に含まれているか否かを表わす情報を発生することを特徴とする。
【００２５】（６）ユーザに渡すディジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、対象を識別する情報として、識別すべき対象が全識別対象の各々であるか否かを表わす情報を発生することを特徴とする。
【００２６】（７）ユーザに渡すディジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、対象を識別する情報として、全識別対象の各々に順位を付け、識別すべき対象が各識別対象より順位が小さいか、等しいか、あるいは大きいかを表わす情報を発生することを特徴とする。
【００２７】（８）（７）に記載の識別情報発生装置において、ディジタルデータを渡す可能性のあるユーザの総数をＮとし、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑそれぞれに対して、ｐを法とした当該ユーザの順位ｎの剰余が０からｐ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報と、ｑを法とした当該ユーザの順位ｎの剰余が０からｑ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報とをユーザを識別する情報として用いることを特徴とする。
【００２８】（９）ディジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、そ

の意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容を記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、識別対象固有の情報に応じて、識別符号を発生する手段と、前記データ割当て部から出力されたデータ変換内容と前記識別符号に応じて、ディジタルデータの所定の部分を変更する識別符号埋め込み手段と、を具備することを特徴とする識別符号埋め込み装置。

【００２９】（１０）ディジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容をその変化程度を表わすコストと共に記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、データ変換後のデータの変化程度を累積する手段と、識別対象固有の情報に応じて、識別符号を発生する手段と、前記データ割当て部から出力されたデータ変換内容と前記識別符号に応じて、ディジタルデータの所定の部分を変更する識別符号埋め込み手段と、前記累積手段により、データの変化程度の累積値が所定の変化程度を超える場合、前記識別符号埋め込み手段の動作を禁止する手段とを具備することを特徴とする識別符号埋め込み装置。

【００３０】（１１）識別情報がユーザには知覚できないように埋め込まれているディジタルデータから識別情報を読み取る識別情報検出装置において、ディジタルデータの所定の位置に埋め込まれている識別符号を抽出する手段と、抽出された識別符号を復号し、識別情報を求める手段と、を具備することを特徴とする。

【００３１】（１２）請求項１に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、ディジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、その部位が請求項１に記載の装置により埋め込まれた、そのユーザ対がこのディジタルデータに対応するユーザを含んでいることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が請求項１に記載の装置により埋め込まれた、そのユーザ対がこのディジタルデータに対応するユーザを含んでいることを表わす符号であると判定されたユーザ対を結託したユーザ対の候補と推定することを特徴とする。

【００３２】（１３）請求項２に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、ディジタルデータから抽出された識別情報から各ユーザに対応する部位を読み取るステップと、その部位が請求項２に記載の装置により埋め込まれた、そのユーザがこのディジタルデータに対応するユーザであることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が請求項２に記載の装置により埋め込まれた、そのユーザがこのディジタルデータに対応するユーザであることを表わす符号であると判定されたユーザを結託したユーザの候補と推定することを特徴とする。

【００３３】（１４）請求項３に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、

１）ディジタルデータから抽出された識別情報から各ユーザに対応する部位を順次読み取るステップと、

２）その部位が請求項３に記載の装置により埋め込まれた、そのユーザの順位がこのディジタルデータに対応するユーザの順位よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ１）、２）を繰り返すステップと、

３）上記ステップ２）において、初めて現れたそれ以外の符号の次の部位から、各ユーザに対応する部位を順次読み取るステップと、

４）その部位が請求項３に記載の装置により埋め込まれた、そのユーザの順位がこのディジタルデータに対応するユーザの順位よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ３）、４）を繰り返すステップと、

５）抽出された識別情報の最後に到達するまで上記ステップ３）、４）、５）を繰り返すステップと、を具備し、上記ステップ２）において、それ以外の符号が初めて現れた部位に対応するユーザを第一の結託ユーザ候補と推定し、上記ステップ４）において、それ以外の符号が最後に現れた部位に対応するユーザを第二の結託ユーザ候補と推定することを特徴とする。

【００３４】（１５）請求項４に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、

１）ディジタルデータから抽出された識別情報からｐを法とするユーザのそれぞれに対応する部位を順次読み取るステップと、

２）その部位が、請求項４に記載の装置により埋め込まれた、ｐを法としたそのユーザの順位の剰余がｐを法としたこのディジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ１）、２）を繰り返すステップと、

３）上記ステップ２）において、初めて現れたそれ以外の符号を次の部位から、ｐを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

４）その部位が、請求項４に記載の装置により埋め込まれた、ｐを法としたそのユーザ順位の剰余がｐを法としたこのディジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号で

あるかを判定し、それ以外の符号が現れるまで、上記ステップ３）、４）を繰り返すステップと、
５）抽出された識別情報からｐを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ３）、４）、５）を繰り返すステップと、
６）上記ステップ５）において、抽出された識別情報からｐを法としたユーザ順位の剰余のすべての部位を読み取った後、その次の部位からｑを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
７）その部位が、請求項４に記載の装置により埋め込まれた、ｑを法としたそのユーザの順位の剰余がｑを法としたこのディジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ６）、７）を繰り返すステップと、
８）上記ステップ７）において、初めて現れたそれ以外の符号を次の部位から、ｑを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
９）その部位が、請求項４に記載の装置により埋め込まれた、ｑを法としたそのユーザ順位の剰余がｑを法としたこのディジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ８）、９）を繰り返すステップと、
１０）抽出された識別情報からｑを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ８）、９）、１０）を繰り返すステップと、を具備し、上記ステップ２）において、それ以外の符号が初めて現れた部位に対応するｐを法としたユーザ順位の剰余と、上記ステップ４）において、それ以外の符号が最後に現れた部位に対応するｐを法としたユーザ順位の剰余と、上記ステップ７）において、それ以外の符号が初めて現れた部位に対応するｑを法としたユーザ順位の剰余と、上記ステップ９）において、それ以外の符号が最後に現れた部位に対応するｑを法としたユーザ順位の剰余とを組み合わせて構成されるｐを法とする剰余とｑを法とする剰余の組に対して中国人剰余定理を適用して結託ユーザの候補を推定することを特徴とする。

【００３５】

【発明の実施の形態】（第１実施形態）以下、図面を参照して本発明による電子透かし埋め込み装置の第１の実施形態を説明する。

【００３６】図１は電子透かし埋め込み装置の第１実施形態の全体のブロック図である。著作物であるディジタルデータ（以下、オリジナルコンテンツと称する）がシンタックス解析部１０、データ変換部１２に供給される。ここで、コンテンツは複数のある意味を持ったひとまとまりのデータから構成されている。以下、このひとまとまりのデータのことを本明細書ではトークンと称する。例えば、ＭＰＥＧビデオの符号化では、トークンとして各種のヘッダーコードやＶＬＣコードなどがある。各トークンがコンテンツ中のどの位置にあって、どういう値を持つかは、そのデータをシンタックス解析することによって分かる。シンタックス解析部１０はオリジナルコンテンツをシンタックス解析することにより、トークンを求める。トークンに関する情報は、データ変換割当て部１４に通知される。データ変換割当て部１４はトークンに応じてデータ変換部１２にデータ変換規則を通知する。

【００３７】ユーザ固有のユーザＩＤが識別符号発生器１６に供給され、当該ユーザ名を特定できる識別符号が発生され、エラー検出／訂正符号化器１８に供給される。エラー検出／訂正符号化器１８はユーザ識別符号をエラー検出／訂正符号化し、データ変換部１２に供給する。なお、このエラー検出／訂正符号化器１８は本発明の必須の構成ではなく、図２に示すように、省略しても構わない。

【００３８】データ変換部１２はデータ変換割当て部１４から通知されたデータ変換指示に従って、コンテンツの所定のビットを識別符号に応じて操作することによりコンテンツに識別符号（電子透かし）を埋め込む。埋め込みの一例は、従来例と同様に、ＭＰＥＧ動画の場合は、ｉ番目のフレームの（ｘ、ｙ）画素の輝度データＶを、埋め込むデータが“１”の場合はＶ＋１とし、埋め込むデータが“０”の場合はそのままとすることにより、埋め込むことが考えられる。

【００３９】図３はデータ変換割当て部１４の具体的な構成を示すブロック図である。データ変換割当て部１４はデータ変換の種々の内容を記憶する状態遷移メモリ２２と、コンテンツの現在の状態を記憶する状態バッファ２６と、コスト評価規則を記憶するコスト評価規則メモリ２８と、コスト累積部２０と、これらを制御するコントローラ２４とからなる。シンタックス解析部１０からのトークンに関する情報はコントローラ２４に供給される。コントローラ２４にはデータ変換部１２からの電子透かし埋め込み後のデータが供給されるとともに、コントローラ２４はデータ変換部１２へ状態遷移メモリ２２から読み出したデータ変換内容を示すデータ変換指示を与える。状態遷移メモリ２２には前提条件毎にデータ変換内容（データ埋め込み規則）、及び変換後の状態である遷移状態、コスト（透かしデータの埋め込みにより、画質等のコンテンツの質の変化、あるいはデータ長の大きな変化等が生じるか否かを判定するための評価基準）を記憶する。状態バッファ２６には、データ変換（透かし埋め込み）処理が行われる毎に、選択されたデータ変換内容に応じた遷移状態がセットされる。コントローラ２４はトークンに応じた前提条件を検索し、対応するデータ変換内容を読み出し、データ変換部１２へ供給する。ただし、コストを考慮して、透かしデータの埋め込

みによりデータが大きく変化することが予想される場合には、データ変換を行わない。このためにコスト評価規則メモリ２８が設けられ、メモリ２８はコスト累積部２０に累積されているコストと、状態遷移メモリ２２の選択したデータ変換内容に対応するコストとを比較し、所定値以上のデータの変化が予想される場合は、データ変換を非実行とする。

【００４０】データ変換部１２は実際に変換したデータに関する情報をコントローラ２４へ返送する。コントローラ２４はそのデータを基にコストを計算し、コスト累積部２０に累積コストを蓄積する。

【００４１】なお、コストによるコンテンツの質の変化判断は本発明の必須の構成ではなく、コスト判断は、省略しても構わない。この場合は、図４に示すように、状態遷移メモリ２２からコストの欄を省略し、コスト累積部２０、コスト評価規則メモリ２８を省略すればよい。

【００４２】第１の実施形態は、従来技術のように、単にユーザが誰であるかを示すだけではなく、ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする。

【００４３】例えば、ディジタルデータがＭＰＥＧ方式の動画像である場合、３人のユーザをユーザＡ、Ｂ、Ｃとし、各ユーザがユーザＡ、Ｂの対に含まれるか否か、ユーザＢ、Ｃの対に含まれるか否か、ユーザＡ、Ｃの対に含まれるか否かを表わす３ビットの識別符号を埋め込む。ユーザＡ、Ｂの対に含まれる場合は１ビット目を“１”とし、ユーザＢ、Ｃの対に含まれる場合は２ビット目を“１”とし、ユーザＡ、Ｃの対に含まれる場合は３ビット目を“１”とし、それ以外は“０”とする。これらの３ビットの識別符号の埋め込み方は、従来例と同様に、１ビット目はｆ１番目のフレームの（ｘ１、ｙ１）画素の輝度データＶ１を、“１”ならばＶ１＋１とし、“０”ならばそのままとし、第２、第３ビット目はｆ２、ｆ３フレームの（ｘ２，ｙ２）画素、（ｘ３，ｙ３）画素の輝度データＶ２、Ｖ３を、“１”ならば＋１とし、“０”ならばそのままとすることにより、埋め込むことができる。

【００４４】このような輝度データの変換はデータ変換部１２で行われる。

【００４５】次に、このような識別符号が埋め込みされたコンテンツをユーザが著作権者に無断で不正にコピーして販売する場合を説明する。従来例と同様に、ユーザＡ、Ｂが結託して、互いのデータを比較して、識別符号を改竄することを試みる。ユーザＡ、Ｂは、両者の差分データであるｆ２フレームの（ｘ２，ｙ２）画素の輝度データＶ２、ｆ３フレームの（ｘ３，ｙ３）画素の輝度データＶ３がユーザＡ固有の透かしデータ、またはユーザＢ固有の透かしデータの一部であると推定でき、これを次のように書換えようとする。

【００４６】（ｆ２；ｘ２，ｙ２）：（Ｖ２、またはＶ２＋１）→Ｖ２＋ΔＶ２

これは、ｆ２フレームの（ｘ２，ｙ２）画素の輝度データＶ２、またはＶ２＋１をＶ２＋ΔＶ２に書換えることを示す。

【００４７】（ｆ３；ｘ３，ｙ３）：（Ｖ３、またはＶ３＋１）→Ｖ３＋ΔＶ３

これは、ｆ３フレームの（ｘ３，ｙ３）画素の輝度データＶ３、またはＶ３＋１をＶ３＋ΔＶ３に書換えることを示す。

【００４８】ΔＶ２、ΔＶ３をどのように選ぶかを考える。

【００４９】（イ）ΔＶ２＝１、ΔＶ３＝０

これは、ユーザＢに埋め込まれる識別符号と同じである。

【００５０】（ロ）ΔＶ２＝０、ΔＶ３＝１

これは、ユーザＡに埋め込まれる識別符号と同じである。

【００５１】（ハ）ΔＶ２＝１、ΔＶ３＝１

これは、結託者はユーザＡ、Ｂ、Ｃの中にいるが、どの２人であるか特定できないことを示す。

【００５２】（ニ）ΔＶ２＝０、ΔＶ３＝０

これは、結託者はユーザＡとＢであることを示す。

【００５３】このため、従来例と同じ推論で、ユーザＡ、Ｂは（イ）、（ロ）の場合は自分達を示す識別情報に書き換わってしまい、ΔＶ１、ΔＶ３をこれ以外のデータに書換えればよいと判断する。そして、ΔＶ１、ΔＶ３を（ハ）、（ニ）のように書換えて、違法コピーを再配布する。しかし、従来例と異なり、（ニ）の場合は、結託者がユーザＡとＢであることが分かってしまう。（ハ）の場合は、結託者を特定できないが、識別符号をＬ回、すなわち、３Ｌ画素に埋め込んでおくと、Ｌ個の識別符号が偶然に全て（ハ）の状態になるのは、（１／２）^{L}の確率であり、現実的には十分有効である。

【００５４】このように第１実施形態によれば、ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を埋め込むことにより、たとえ複数のユーザが結託して、差分データを改竄して、自分達のデータ以外のデータに書換えても、改竄後のデータに自分達の対を示すデータが残ってしまうので、結託が失敗に終わる。

【００５５】なお、本発明は識別符号としては、ユーザ名を識別する情報に限らず、一般的な対象を識別する情報をユーザに渡すディジタルデータに、ユーザには知覚できないように付加する場合にも適用できる。例えば、ユーザにその存在は知覚できるが、その符号の意味を教えていない形で、メッセージの一部として授受することができる。また、ユーザ名の識別以外の情報としては、

利用の日付、日時、利用者端末の識別、ディジタルデータの識別、ディジタルデータの転送経路の識別、利用の条件の記述等としても利用できる。

【００５６】図５は第１実施形態の識別符号の発生アルゴリズムを示す図である。このアルゴリズムは、ユーザ名識別符号以外の一般的な識別符号に対しても適用できる。ステップＳ２で、識別対象部分集合（ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対）ｐ１、ｐ２、…ｐｍａｘに便宜上の順序を与える（ｐ１＜ｐ２…＜ｐｍａｘ）。ステップＳ４で、識別対象であるユーザｕを特定する。ステップＳ６で、変数ｉに１をセットし、codeの初期値としてビット長０の初期値をセットする。ステップＳ８で、当該ユーザｕが部分集合ｐｉに含まれているか否かを判定する。含まれている場合は、ステップＳ１０で識別符号のビットcode(ｕ∈ｐｉ)（＝１：第１実施形態の場合）を発生し、今までの識別符号に連接する。含まれていない場合には、ステップＳ１２で識別符号のビットcode(ｕ≠ｐｉ)（＝０：第１実施形態の場合）を発生し、今までの識別符号に連接する。ステップＳ１０、Ｓ１２で発生される符号は１ビットに限らず、複数ビットでもよい。記号≠は集合に属さない（∈の否定）を表わす。この後、ステップＳ１４で変数ｉがｍａｘ（部分集合の総数）以上か否かを判定する。ノーの場合は、ステップＳ１６で変数ｉをインクリメント（＋１）して、ステップＳ８に戻り、当該ユーザｕが次の部分集合ｐｉに含まれているか否かを判定する。ステップＳ１４でイエスの判定が得られた場合は、全ての部分集合ｐｉに対して当該ユーザｕがその部分集合に含まれるか否かの判定が終了し、識別符号の各ビットの発生、連接が終了したとして、動作終了する。

【００５７】図６は、不正コピーと思えるコンテンツが流通し、コンテンツから透かしデータを抽出し、不正を働いたであろうユーザを識別するために用いられる透かし抽出装置の一例である。透かしデータの埋め込み位置を知るために、図１の透かし埋め込み装置と同様に、オリジナルコンテンツがシンタックス解析部４０に供給され、トークンに関する情報がデータ変換割当て部４２に入力される。データ変換割当て部４２はトークンから透かしデータの埋め込み位置と変換内容を示す変換内容情報を発生する。なお、オリジナルコンテンツ毎に透かし埋め込み位置と変換内容は決まっているので、変換内容情報はトークンから毎回求めなくても良く、一度求めておいて、コンテンツ毎にメモリ等に格納しておいて、読み出す構成にしても良い。その場合、シンタックス解析部４０とデータ変換割当て部４２の代わりにメモリを設けることになる。

【００５８】透かし埋め込み済みコンテンツと、データ変換割当て部４２からの変換内容情報とが識別符号抽出部４４に供給される。識別符号抽出部４４は変換内容情報に応じてコンテンツから埋め込まれている識別符号を抽出する。抽出された識別符号はエラー検出／訂正復号器４６を介して、識別符号復号器４８に供給され、識別符号に応じてユーザＩＤが検出される。透かし埋め込み装置側にエラー検出／訂正符号化器１８が設けられていない場合には、エラー検出／訂正復号器４６は省略される。エラー検出／訂正復号器４６が設けられない場合の透かし抽出装置を図７に示す。

【００５９】図８は第１実施形態の識別符号復号器４８のアルゴリズムを示す。ステップＳ２０２で、識別対象部分集合（ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対）ｐ１、ｐ２、…ｐｍａｘに埋め込み時と同じ順序を与える（ｐ１＜ｐ２＜…＜ｐｍａｘ）。ステップＳ２０４で、codeの初期値として入力された抽出符号をセットする。ステップＳ２０６で、変数ｉに１をセットし、結託者のユーザ対の候補であるcandidate-pairs に全部のユーザ対の集合｛ｐ１、ｐ２、…ｐｍａｘ｝をセットする。

【００６０】ステップＳ２０８で、codeの先頭の符号が１か否かを判定する。１である場合は、すぐにステップＳ２１２へ進む。１ではない場合は、ステップＳ２１０でcandidate-pairs からユーザ対ｐｉを取り除いてから、ステップＳ２１２へ進む。ステップＳ２１２では、変数ｉがｍａｘ（部分集合の総数）以上か否かを判定する。ノーの場合は、ステップＳ２１４で変数ｉをインクリメント（＋１）し、ステップＳ２１６でcodeを１ビット左へシフトし、ステップＳ２０８のcodeの先頭の符号の判定に戻る。ステップＳ２１２でイエスの判定が得られた場合は、動作終了する。この後、candidate-pairs に残っているユーザ対Ｐが結託者対であると推測される。

【００６１】図８のアルゴリズムの特徴をまとめると、１）ディジタルデータから抽出された識別符号から各ユーザ対ｐｉに対応する部位を読み取り、２）その部位が図５のアルゴリズムで埋め込まれた符号$code_u$（ｕ∈ｐｉ）であるか、それ以外の符号であるかを判定し、３）上記２）において、$code_u$（ｕ∈ｐｉ）であると判定されたユーザ対ｐｉを結託したユーザ対の可能性があると推測できる。

【００６２】識別符号がＬ回埋め込まれた場合は、上記のアルゴリズムをＬ回行い、各アルゴリズムの実行時に、常にcandidate-pairs に残っているユーザ対Ｐが結託者対である可能性が高いと推測される。

【００６３】第１実施形態ではユーザ数をＮとすると、任意のユーザ対からなる部分集合の総数は全部でＮＣ２となり、識別符号の符号量はＮ２のオーダとなり、ｌｏｇ２Ｎのオーダであった従来例に比べて、複数のユーザの結託には強いが、符号量が増える。

【００６４】そこで、識別符号の符号量が増大すること無く、しかもユーザの結託による改竄に強い透かしデー

タ埋め込みの他の実施形態を説明する。他の実施形態の説明において第１の実施形態と同一部分は同一参照数字を付してその詳細な説明は省略する。他の実施形態の装置構成は第１実施形態と同じであるので、構成を示すブロック図、およびその説明は省略する。

【００６５】（第２実施形態）第２の実施形態は、当該ユーザがディジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を論理積（記号∩で表わす）の形で連接して用いることを特徴とする。例えば、ユーザu_iに対しては、ユーザu_1～u_{i-1}ではなく、ユーザu_iであり、かつユーザu_{i+1}～u_Nではないという論理的な意味を持つ次のようなデータを埋め込む。

【００６６】$\neg u_1 \cap \neg u_2 \cap \cdots \cap \neg u_{i-1} \cap u_i \cap \neg u_{i+1} \cap \neg u_{i+2} \cap \cdots \cap \neg u_N$

ここで、¬は否定を表わし、$\neg u_1$はユーザu_1ではないということを示すデータである。

【００６７】具体的に埋め込むデータの符号を上の論理式のＡＮＤ（∩）をとっている個々の項に対応して割り当てる。

【００６８】$\neg u_i \rightarrow code_i(\neg u_i)$

$u_i \rightarrow code_i(u_i)$

埋め込むべき識別符号は個々の項に割り当てた符号を連接（記号‖で表わす）して作ることにする。連接の順序は本実施形態では本質とは無関係であるが、説明の便宜上、ここではユーザに対応する添え字の順序とする。

【００６９】ユーザu_1に埋め込む識別符号：

$code_1(u_1) \| code_1(\neg u_2) \| code_1(\neg u_3) \| \cdots \| code_1(\neg u_N)$

ユーザu_2に埋め込む識別符号は

$code_2(\neg u_1) \| code_2(u_2) \| code_2(\neg u_3) \| \cdots \| code_2(\neg u_N)$

ユーザu_3に埋め込む識別符号は

$code_3(\neg u_1) \| code_3(\neg u_2) \| code_3(u_3) \| \cdots \| code_3(\neg u_N) \cdots$

ユーザu_iに埋め込む識別符号は

$code_i(\neg u_1) \| code_i(\neg u_2) \| code_i(\neg u_3) \| \cdots \| code_i(\neg u_{i-1}) \| code_i(u_i) \| code_i(\neg u_{i+1}) \| \cdots \| code_i(\neg u_N) \cdots$

ユーザu_Nに埋め込む識別符号は

$code_N(\neg u_1) \| code_N(\neg u_2) \| code_N(\neg u_3) \| \cdots \| code_N(\neg u_{N-1}) \| code_N(u_N)$

ここで、例えば、$code_i(u_j)$は“１”、$code_i(\neg u_j)$は“０”とする。

【００７０】図９は第２実施形態の識別符号の発生アルゴリズムを示す図である。このアルゴリズムも、ユーザ名識別符号以外の一般的な識別符号に対しても適用できる。ステップＳ２２で、全識別対象（ディジタルデータを渡す可能性のある全ユーザ）u_1、u_2、…u_{max}に便宜上の順序を与える（$u_1 < u_2 < \cdots < u_{max}$）。ステップＳ２４で、識別対象であるユーザ$u_i$を特定する。ステップＳ２６で、変数ｊに１をセットし、codeに初期値（ビット長：０）をセットする。ステップＳ２８で、変数ｊがユーザu_iを示すパラメータｉと等しいか否かを判定する。等しい場合は、ステップＳ３０で識別符号の１ビット$code_i(u_j)$（＝“１”）を発生し、今までの識別符号に連接する。等しくない場合には、ステップＳ３２で識別符号の１ビット$code_i(\neg u_j)$（＝“０”）を発生し、今までの識別符号に連接する。この後、ステップＳ３４で変数ｊがｍａｘ（ユーザの総数）以上か否かを判定する。ノーの場合は、ステップＳ３６で変数ｊをインクリメント（＋１）して、ステップＳ２８に戻り、変数ｊがｉに等しいか否かを判定する。ステップＳ３４でイエスの判定が得られた場合は、全てのユーザに対して当該ユーザu_iがそのユーザに等しいか否かの判定が終了し、識別符号の各ビットの発生、連接が終了したとして、動作終了する。

【００７１】次に、このような識別符号が埋め込みされたコンテンツをユーザが著作権者に無断で不正にコピーして販売する場合を説明する。ユーザu_iとu_jが結託すると、ユーザu_iのデータの中の$code_i(u_i)$と$code_i(\neg u_j)$がユーザu_jのデータの中の$code_j(\neg u_i)$と$code_j(u_j)$と違うので、これらを書換えることを考える。

【００７２】すなわち、$code_i(u_i)$と$code_i(\neg u_j)$を$code_i'$に、$code_j(\neg u_i)$と$code_j(u_j)$を$code_j'$に書換えることになるが、書き換えの態様は次の態様が考えられる。

【００７３】（イ）$code_i' = code_i(u_i)$, $code_j' = code_i(\neg u_j)$

これは、ユーザu_iに埋め込まれる識別符号と同じである。

【００７４】（ロ）$code_i' = code_j(\neg u_i)$, $code_j' = code_j(u_j)$

これは、ユーザu_jに埋め込まれる識別符号と同じである。

【００７５】（ハ）$code_i' = code_i(u_i)$, $code_j' = code_j(u_j)$

これは、結託者はユーザu_iとu_jがであることを示す。

【００７６】（ニ）$code_i' = code_j(\neg u_i)$, $code_j' = code_i(\neg u_j)$

この場合は、結託者を特定できない。

【００７７】（ホ）$code_i' \neq code_i(u_i) \neq code_j(\neg u_i)$, $code_j' =$ ****

これは、ユーザu_iが結託に参加していることを示す。

【００７８】（ヘ）$code_i' =$ ****, $code_j' \neq code_j(u_j) \neq code_i(\neg u_j)$

これは、ユーザu_jが結託に参加していることを示す。

【００７９】このため、従来例と同じ推論で、ユーザＡ、Ｂは（イ）、（ロ）の場合は自分達を示す識別情報

に書き換わってしまい、これ以外の書き換えを行えばよいと判断する。そして、（ハ）、（ニ）、（ホ）、（ヘ）のように書換えて、違法コピーを再配布する。しかし、従来例と異なり、（ハ）の場合は、結託者がユーザｕｉとｕｊがであることが分かってしまうし、（ホ）、（ヘ）の場合も、ユーザｕｉ、またはｕｊが結託者の１人であることが分かってしまう。また、（ニ）の場合は結託者を特定できないが、第１実施形態と同様に識別符号をＬ回埋め込むことにより、Ｌ個の識別符号が偶然に全て（ニ）の状態になるのは、（１／４）Ｌの確率であり、現実的には十分有効である。

【００８０】図１０は第２実施形態の識別符号復号器４８のアルゴリズムを示す。ステップＳ２２２で、識別対象（ユーザ）ｕ１、ｕ２、…ｕｍａｘに埋め込み時と同じ順序を与える（ｕ１＜ｕ２＜…＜ｕｍａｘ）。ステップＳ２２４で、codeの初期値として入力された抽出符号をセットする。ステップＳ２２６で、変数ｉに１をセットし、結託ユーザの候補の集合である集合candidatesに空集合｜｜をセットする。

【００８１】ステップＳ２２８で、codeの先頭はあるｊに対するcodej（￢ｕｉ）であるか否かを判定する。イエスの場合は、すぐにステップＳ２３２に進み、ノーの場合は、ステップＳ２３０で集合candidatesにユーザｕｉを加えてから、ステップＳ２３２に進む。ステップＳ２３２では、変数ｉがｍａｘ（ユーザの総数）以上か否かを判定する。ノーの場合は、ステップＳ２３４で変数ｉをインクリメント（＋１）し、ステップＳ２３６でcodeをcodej（￢ｕｉ）の長さ（ビット数）だけ左へシフトし、ステップＳ２２８のcodeの先頭の判定に戻る。ステップＳ２３２でイエスの判定が得られた場合は、動作終了する。この後、集合candidatesに含まれているユーザが結託者であると推測される。

【００８２】図１０のアルゴリズムをまとめると、１）ディジタルデータから抽出された識別符号から各識別対象ｕｉに対応する部位を読み取り、２）その部位が図９のアルゴリズムで埋め込まれた符号codei（ｕｊ）であるか、それ以外の符号であるかを判定し、３）上記２）で符号codei（ｕｊ）であると判定されたユーザを結託したユーザの可能性があると推測できる。

【００８３】識別符号がＬ回埋め込まれた場合は、上記のアルゴリズムをＬ回行い、各アルゴリズムの実行時に、candidatesに含まれているユーザが結託者である可能性が高いと推測される。

【００８４】このように第２実施形態によれば、当該ユーザがディジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を論理積の形で連接した識別符号を埋め込むことにより、たとえ複数のユーザが結託して、差分データを改竄して、自分達のデータ以外のデータに書換えても、改竄後のデータに自分達が結託に関与したことを示すデータが残ってしまうので、結託が失敗に終わる。

【００８５】第２実施形態の識別符号の符号量はオーダＮの量であり、第１実施形態より符号量を大幅に削減することができる。

【００８６】（第３実施形態）第２実施形態は３人以上のユーザの結託には弱い。

【００８７】ユーザｕｉ、ｕｊ、ｕｋが結託する場合を考える。

【００８８】ユーザｕｉに埋め込む識別符号：
…‖codei（ｕｉ）‖…‖codei（￢ｕｊ）‖…‖codei（￢ｕｋ）‖…
ユーザｕｊに埋め込む識別符号：
…‖codej（￢ｕｉ）‖…‖codej（ｕｊ）‖…‖codej（￢ｕｋ）‖…
ユーザｕｋに埋め込む識別符号：
…‖codek（￢ｕｉ）‖…‖codek（￢ｕｊ）‖…‖codek（ｕｋ）‖…
ユーザｕｉ、ｕｊのデータの差分データからcodei（ｕｉ、または￢ｕｉ）とcodej（ｕｊ、または￢ｕｊ）の部位P_{ij}が特定できる。ただし、各点がどちらに属するのかは分からない。同様に、ユーザｕｊ、ｕｋのデータの差分データからcodej（ｕｊ、または￢ｕｊ）とcodek（ｕｋ、または￢ｕｋ）の部位P_{jk}が特定できる。ただし、各点がどちらに属するのかは分からない。

【００８９】これらの部分集合から、次のようにしてｕｉ、ｕｊ、ｕｋそれぞれの部位Ｐｉ、Ｐｊ、Ｐｋが特定できる。

【００９０】

$$P_{ij} \cap \ /P_{jk} \rightarrow \{code_i\ (u_i\ 、または\neg u_i\ )\ の部位\}\ P_i$$
$$= P_{ij} - P_{jk}$$

ここで、記号「／」は補集合を表わす。例えば、Ｐがデータ中のある部位とすると、／Ｐはデータ中のＰ以外の部分である。

【００９１】

$$P_{jk} \cap \ /P_{ij} \rightarrow \{code_k\ (u_k\ 、または\neg u_k\ )\ の部位\}\ P_k$$
$$= P_{jk} - P_{ij}$$
$$P_{ij} \cap /P_i \rightarrow \{code_i\ (u_j\ 、または\neg u_i\ )\ の部位\}\ P_j$$
$$= P_{ij} - P_i$$

この結果、次のことが分かる。

【００９２】ｕｉの埋め込みデータのＰｉの部分はcodei（ｕｉ）を表わす。ｕｉの埋め込みデータのＰｉの部分はcodei（￢ｕｉ）を表わす。これにより、codei（ｕｉ）、codei（￢ｕｉ）が分かってしまう。

【００９３】同様にして、codej（ｕｊ）、codej（￢

ｕｊ）、codek （ｕｋ）、codek （¬ｕｋ）が分かってしまう。

【００９４】このため、結託者はcodei （¬ｕｉ）、codej （¬ｕｊ）、codek （¬ｕｋ）をＰｉ、Ｐｊ、Ｐｋに書き込むと、誰のものでもないデータを生成できてしまう。

【００９５】このような３人以上の結託に対しても強くするために、ユーザの集合に次のように整列順序を付す。これは、コンテンツの提供者が決めればよい。

【００９６】ｕ１＜ｕ２＜…＜ｕｉ-１＜ｕｉ＜ｕｉ+１＜…＜ｕｊ-１＜ｕｊ＜ｕｊ+１＜…＜ｕＮ

順序を付す理由は、結託に加わったユーザを最小値、最大値とする部分集合を特定できるようにすることである。例えば、部分集合ｕｉ＜ｕｉ+１＜…＜ｕｊ-１＜ｕｊが特定されると、結託に加わったユーザはユーザｕｉ、ｕｊ、その他であることが分かる。

【００９７】ユーザｕ１に埋め込む識別符号：

code１（ｕ１）‖code１（¬ｕ２）‖code１（¬ｕ３）‖…‖code１（¬ｕＮ）

ユーザｕ２に埋め込む識別符号は

code２（¬ｕ１）‖code２（ｕ２）‖code２（¬ｕ３）‖…‖code２（¬ｕＮ）

ユーザｕ３に埋め込む識別符号は

code３（¬ｕ１）‖code３（¬ｕ２）‖code３（ｕ３）‖…‖code３（¬ｕＮ）…

ユーザｕｉに埋め込む識別符号は

codei（¬ｕ１）‖codei（¬ｕ２）‖codei（¬ｕ３）‖…‖codei（¬ｕi-１）‖codei（ｕｉ）‖codei（¬ｕi+１）‖…‖codei（¬ｕＮ）…

ユーザｕＮに埋め込む識別符号は

codeＮ（¬ｕ１）‖codeＮ（¬ｕ２）‖codeＮ（¬ｕ３）‖…‖codeＮ（¬ｕN-１）‖codeＮ（ｕＮ）

一般的に、ユーザｕｉに埋め込む識別符号において、codei（ｕｉ）より前のcodei（¬ｕ１）‖codei（¬ｕ２）‖…‖codei（¬ｕi-１）は、ここには結託者はいない（ｉ番目より順位の小さいユーザは結託に参加していない）ことを示す。同様に、codei（ｕｉ）より後のcodei（¬ｕi+１）‖…‖codei（¬ｕＮ）も、ここには結託者はいない（ｉ番目より順位の大きいユーザは結託に参加していない）ことを示す。すなわち、第３実施形態では、対象を識別する情報として、全識別対象の各々に順位を付け、識別すべき対象が各識別対象より順位が小さいか、等しいか、あるいは大きいかを表わす情報を用いる。

【００９８】ユーザｕｉ、ｕｊに埋め込む識別符号に関しては、場所によって符号の意味が異なるものには、異なる符号を割り当てる。例えば、ｉ番目のデータは、ユーザｕｉに埋め込む識別符号に対しては、このデータはｕｉのものであることを意味し、ユーザｕｊに埋め込む識別符号に対しては、ｕｉより小さいユーザに結託者はいないことを意味する。また、ｋ（ｉ＜ｋ＜ｊ）番目のデータは、ユーザｕｉに埋め込む識別符号に対しては、ｕｋより大きいユーザに結託者はいないことを意味し、ユーザｕｊに埋め込む識別符号に対しては、ｕｋより小さいユーザに結託者はいないことを意味する。

【００９９】これを考慮すると、次のような符号を割当てることが考えられる。

【０１００】

code１（ｕ１）≠code２（¬ｕ１）＝code３（¬ｕ１）＝…＝codeＮ（¬ｕ１）

code１（¬ｕ２）≠code２（ｕ２）≠code３（¬ｕ２）＝…＝codeＮ（¬ｕ２）

code１（¬ｕ３）＝code２（¬ｕ３）≠code３（ｕ３）≠code４（¬ｕ３）＝…＝codeＮ（¬ｕ３）

…

ここで、等しいcodeは同一の変数を用いると、全部で３つの変数ａ、ｂ、ｃ用いて、次のように識別符号を表わすことができる。

【０１０１】

ユーザｕ１に埋め込む識別符号：$a^{(1)}$ $b^{(2)}$ $b^{(3)}$ ……$b^{(N)}$

ユーザｕ２に埋め込む識別符号：$c^{(1)}$ $a^{(2)}$ $b^{(3)}$ ……$b^{(N)}$

ユーザｕｉに埋め込む識別符号：$c^{(1)}$ $c^{(2)}$ $c^{(3)}$ …$a^{(i)}$ ……$b^{(N)}$

ユーザｕＮに埋め込む識別符号：$c^{(1)}$ $c^{(2)}$ $c^{(3)}$ ……$c^{(N-1)}$ $a^{(N)}$

図１１は第３実施形態の識別符号の発生アルゴリズムを示す図である。このアルゴリズムも、ユーザ名識別符号以外の一般的な識別符号に対しても適用できる。ステップＳ４２で、全識別対象（ディジタルデータを渡す可能性のある全ユーザ）ｕ１、ｕ２、…ｕＮに順序を与える（ｕ１＜ｕ２＜…＜ｕＮ）。ステップＳ４４で、識別対象であるユーザｕｉを特定する。ステップＳ４６で、変数ｊに１をセットし、codeに初期値（ビット長：０）をセットする。

【０１０２】ステップＳ４８で、変数ｊがユーザｕｉを示すパラメータｉと等しいか否かを判定する。等しい場合は、ステップＳ５０で識別符号の１ビット$a^{(j)}$を発生し、今までの識別符号に連接する。等しくない場合には、ステップＳ５２で変数ｊがユーザｕｉを示すパラメータｉより小さいか否かを判定する。小さい場合は、ステップＳ５４で識別符号の１ビット$c^{(j)}$を発生し、今

までの識別符号に連接する。小さくない場合には、ステップＳ５６で、識別符号の１ビット$b^{(j)}$を発生し、今までの識別符号に連接する。

【０１０３】この後、ステップＳ５８で変数ｊがＮ（ユーザの総数）以上か否かを判定する。ノーの場合は、ステップＳ６０で変数ｊをインクリメント（＋１）して、ステップＳ４８に戻り、変数ｊがｉに等しいか否かを判定する。ステップＳ５８でイエスの判定が得られた場合

ユーザu_iに埋め込む識別符号：

$c^{(1)} \cdots c^{(i-1)}\ a^{(i)}\ b^{(i+1)} \cdots\cdots b^{(N)}$

ユーザu_jに埋め込む識別符号：

$c^{(1)} \cdots\ c^{(j-1)}\ a^{(j)}\ b^{(j+1)} \cdots\cdots b^{(N)}$

ユーザu_kに埋め込む識別符号：

$c^{(1)} \cdots\ c^{(k-1)}\ a^{(k)}\ b^{(k+1)} \cdots\cdots b^{(N)}$

３人のユーザが結託に成功するためには次のような識別符号が得られる必要がある。

$c^{(1)} \cdots c^{(i-1)}\ *^{(i)}\ *^{(i+1)} \cdots *^{(k-1)}\ *^{(k)}\ b^{(k+1)} \cdots\cdots b^{(N)}$

この$*^{(i)}\ *^{(i+1)} \cdots *^{(k-1)}\ *^{(k)}$の部分集合が結託者を特定するので、最小値$*^{(i)}$が$a(i)$ではユーザ$u_i$が結託に参加していることが分かってしまう。そのため、$*^{(i)} = c^{(i)}$としてユーザu_iは結託に参加していないことにしないといけない。また、$*^{(i)} = b^{(i)}$、その他のコードではユーザu_iが結託に参加していることになってしまう。ユーザu_iの識別符号の部位P_iが特定できれば、ユーザu_kのデータから、$*^{(i)} = c^{(i)}$とするのは容易である。しかし、特定できるのは、$P_i \cdots P_{j-1}$（$P_{ij}-P_{jk}$）という全体であり、部位P_iは特定できない。

【０１０７】同様に、最大値$*^{(k)}$が$a^{(k)}$ではユーザu_kが結託に参加していることが分かってしまう。そのため、$*^{(k)} = b^{(k)}$としてユーザu_kは結託に参加していないことにしないといけない。また、$*^{(k)} = c^{(k)}$、その他のコードではユーザu_kが結託に参加していることになってしまう。ユーザu_kの識別符号の部位P_kの部分が特定できれば、ユーザu_iのデータから、$*^{(k)} = b^{(k)}$とするのは容易である。しかし、特定できるのは、$P_{j+1} \cdots P_k$（$P_{jk}-P_{ij}$）という全体であり、部位P_kは特定できない。

【０１０８】ランダムな操作により$*^{(i)} = c^{(i)}$、かつ$*^{(k)} = b^{(k)}$とするには偶然に頼るしかなく、それぞれの確率を$p^{(i)}$、$p^{(k)}$とすると、結託が成功する確率は$p^{(i)} \times p^{(k)}$となり、一般に、$p^{(i)} \leqq 1/2$、$p^{(k)} \leqq 1/2$であって、特に、$c^{(i)}$と$b^{(k)}$の符号長がある程度長い場合には、$p^{(i)}$と$p^{(k)}$は１より十分小さいので、結託が成功する確率は小さいと言える。さらに、上記実施形態と同様に、識別情報をＬ回埋め込むことにより、この確率を$(p^{(i)} \times p^{(k)})^L$と、さらに小さくすることができる。

【０１０９】図１２は第３実施形態の識別符号復号器４８のアルゴリズムを示す。ステップＳ２４２で、識別対は、全てのユーザに対して当該ユーザu_iがそのユーザに等しいか否かの判定が終了し、識別符号の各ビットの発生、連接が終了したとして、動作終了する。

【０１０４】次に、このような識別符号を埋め込むことにより、３人のユーザu_i、u_j、u_kが結託したとしても、結託が成功しない理由を説明する。

【０１０５】

【０１０６】

象（ユーザ）u_1、u_2、$\cdots u_N$に埋め込み時と同じ順序を与える（$u_1 < u_2 < \cdots < u_N$）。ステップＳ２４４で、変数ｉに１をセットし、codeの初期値として入力された抽出符号をセットし、第１の結託者の候補であるcandidate １に１をセットし、第２の結託者の候補であるcandidate ２に１をセットする。ステップＳ２４６で、codeの先頭が$c^{(i)}$であるか否かを判定する。イエスの場合は、ステップＳ２４８で変数ｉをインクリメント（＋１）し、ステップＳ２５０で第１の結託者の候補であるcandidate １、及び第２の結託者の候補であるcandidate ２をそれぞれインクリメント（＋１）する。ステップＳ２５２でcodeを$c^{(i)}$の長さだけ左へシフトし、ステップＳ２４６のcodeの先頭の判定に戻る。ここで、$c^{(i)}$の長さを$|c^{(i)}|$と表わし、$|a^{(i)}| = |b^{(i)}| = |c^{(i)}|$とする。ステップＳ２４６でノーの判定が得られた場合は、ステップＳ２５４で変数ｉをインクリメント（＋１）し、codeを$c^{(i)}$の長さだけ左へシフトし、ステップＳ２５６で、codeの先頭が$b^{(i)}$であるか否かを判定する。ノーの場合は、ステップＳ２５８で第２の結託者の候補であるcandidate ２に変数ｉを代入し、ステップＳ２５４へ戻る。ステップＳ２６０でイエスの判定が得られた場合は、動作終了する。この後、candidate １、candidate ２が結託者の中の２人であると推測される。

【０１１０】図１２のアルゴリズムの特徴をまとめると、１）ディジタルデータから抽出された識別符号を先頭から順次、各識別対象u_iに対応する部位を読み取り、２）その部位が、図１１のアルゴリズムで埋め込まれた符号$c^{(i)}$であるか、それ以外の符号であるかを判定し、$c^{(i)}$以外の符号が現われるまで、上記１）、２）を繰り返し、３）上記２）において初めて$c^{(i)}$以外の符号が現われたときの、ｉを結託ユーザの候補の一人であると判定し、４）上記２）において初めて現われ

たｃ$^{(i)}$ 以外の符号の次の部位から、各識別対象ｕｉに対応する部位を読み取り、５）その部位が、図１１のアルゴリズムで埋め込まれた符号ｂ$^{(i)}$ であるか、それ以外の符号であるかを判定し、ｂ$^{(i)}$ 以外の符号が現われるまで、上記４）、５）を繰り返し、６）上記５）においてｂ$^{(i)}$ 以外の符号が現われたときの、ｉが結託ユーザのもう一人の候補であると「仮に」判定し、７）抽出された識別符号の最後に到達するまで上記４）、５）、６）を繰返し、８）抽出された識別符号の最後に到達した時点での結託ユーザのもう一人の候補として「仮に」判定されているユーザをもう一人の結託ユーザであると判定する。

【０１１１】識別符号がＬ回埋め込まれた場合は、上記のアルゴリズムをＬ回行い、各アルゴリズムの実行時に、candidate １、candidate ２が結託者である可能性が高いと推測される。

【０１１２】第３実施形態の識別符号の符号量もオーダＮの量であり、第１実施形態より符号量を大幅に削減することができる。

【０１１３】結託攻撃に対する電子透かしの従来例として、「結託攻撃に強い電子透かし法」鈴置昌宏等、SCIS'97 The 1997 Symposium on Cryptography and InformationSecurity と"Collusion-Secure Fingerprinting for Digital Data", D. Bonehand J. Shaw, Advances in Cryptology Proceedings of CRYPTO'95, pp257-270(1994)があるが、鈴置等の例は、ａ＝００、ｂ＝１０、ｃ＝０１に相当し、Boneh et al.の例は、ａ、ｂ、ｃはＬ（任意の正整数）ビットであり、ａａ＝ｂ＝００…０（全て０）、ｃ＝１１…１（全て１）に相当する。すなわち、第３実施形態はこれらの方法よりも、一般的な符号化であると言える。

【０１１４】（第４実施形態）さらに、符号量を削減する実施形態を説明する。この実施形態は、中国人剰余定理を応用するものである。中国人剰余定理とは、互いに素な整数ｐ１、ｐ２、…ｐｋ（これらの整数はｎ≦ｐ１×ｐ２×…×ｐｋという関係を満たす）があった時、ｎ１＝ｎmod ｐ１、ｎ２＝ｎmod ｐ２、…ｎｋ＝ｎmod ｐｋというｎ１、ｎ２、…ｎｋからｎが一意的に求められるという定理である。これを応用（Ｎ≦ｐ×ｑとする）すると、１～ｐの中のｒ番目と、１～ｑの中のｓ番目のユーザを特定することにより、第３実施形態のユーザ数Ｎの全ユーザの集合中のｎ番目のユーザを特定することができる。ユーザ数ｐとｑの２つの集合中のそれぞれｒ（＝ｎmod ｐ）、ｓ（＝ｎmod ｑ）番目のユーザを特定する識別符号の方がユーザ数Ｎの全ユーザの集合中のｎ番目のユーザを特定する識別符号よりも符号量が少なくて済む。

【０１１５】第４実施形態において、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑを定義し、ユーザを特定するパラメータｉ（ｉ＝１～Ｎ）の代わりに、パラメータｒ（１～ｐ）およびｓ（１～ｑ）により各ユーザを特定する。説明の便宜上、ｐ＝７、ｑ＝５とする。

【０１１６】ユーザｕ１ に埋め込む識別符号：
ａ$^{(1)}$ ｂ$^{(2)}$ ｂ$^{(3)}$ ｂ$^{(4)}$ ｂ$^{(5)}$ ｂ$^{(6)}$ ｂ$^{(7)}$ ａ$^{(1)}$ ｂ$^{(2)}$ ｂ$^{(3)}$ ｂ$^{(4)}$ ｂ$^{(5)}$
ユーザｕ２ に埋め込む識別符号：
ｃ$^{(1)}$ ａ$^{(2)}$ ｂ$^{(3)}$ ｂ$^{(4)}$ ｂ$^{(5)}$ ｂ$^{(6)}$ ｂ$^{(7)}$ ｃ$^{(1)}$ ａ$^{(2)}$ ｂ$^{(3)}$ ｂ$^{(4)}$ ｂ$^{(5)}$…
ユーザｕ６ に埋め込む識別符号：
ｃ$^{(1)}$ ｃ$^{(2)}$ ｃ$^{(3)}$ ｃ$^{(4)}$ ｃ$^{(5)}$ ａ$^{(6)}$ ｂ$^{(7)}$ ａ$^{(1)}$ ｂ$^{(2)}$ ｂ$^{(3)}$ ｂ$^{(4)}$ ｂ$^{(5)}$
ユーザｕ７ に埋め込む識別符号：
ｃ$^{(1)}$ ｃ$^{(2)}$ ｃ$^{(3)}$ ｃ$^{(4)}$ ｃ$^{(5)}$ ｃ$^{(6)}$ ａ$^{(7)}$ ｃ$^{(1)}$ ａ$^{(2)}$ ｂ$^{(3)}$ ｂ$^{(4)}$ ｂ$^{(5)}$
ユーザｕ８ に埋め込む識別符号：
ａ$^{(1)}$ ｂ$^{(2)}$ ｂ$^{(3)}$ ｂ$^{(4)}$ ｂ$^{(5)}$ ｂ$^{(6)}$ ｂ$^{(7)}$ ｃ$^{(1)}$ ｃ$^{(2)}$ ａ$^{(3)}$ ｂ$^{(4)}$ ｂ$^{(5)}$…
上の符号の前半部分＊$^{(1)}$ ＊$^{(2)}$ ＊$^{(3)}$ ＊$^{(4)}$ ＊$^{(5)}$ ＊$^{(6)}$ ＊$^{(7)}$ はｒに関する符号部分codeｒであり、後半部分＊$^{(1)}$ ＊$^{(2)}$ ＊$^{(3)}$ ＊$^{(4)}$ ＊$^{(5)}$ はｓに関する符号部分codeｓである。それぞれ、符号ａの位置がｒ、ｓの値を示す。なお、ｒに関する符号部分に含まれる符号ａ、ｂ、ｃと後半部分に含まれる符号ａ、ｂ、ｃは同じ物である必要は無く、後半部分に含まれる符号はｄ、ｅ、ｆでもよい。

【０１１７】図１３、図１４は第４実施形態の識別符号の発生アルゴリズムを示す図である。このアルゴリズムも、ユーザ名識別符号以外の一般的な識別符号に対しても適用できる。ステップＳ６４で、全識別対象（ディジタルデータを渡す可能性のある全ユーザ）ｕ１、ｕ２、…ｕＮ（ｕ１＜ｕ２＜…＜ｕＮ）に順序を与える。ステップＳ６６で、識別対象であるユーザｕｉを特定する。ステップＳ６８で、Ｎ≦ｐ×ｑを満たす互いにその整数ｐ、ｑを求める。ステップＳ７０で、変数ｊに１をセットし、codeｒに初期値（ビット長：０）をセットする。ステップＳ７２で、変数ｊがｉmod ｐと等しいか否かを判定する。等しい場合は、ステップＳ７４で識別符号codeｒの１ビットａ$^{(j)}$ を発生し、今までの識別符号codeｒに連接する。等しくない場合には、ステップＳ７６で変数ｊがｉmod ｐより小さいか否かを判定する。小さい場合は、ステップＳ７８で識別符号codeｒの１ビットｃ$^{(j)}$ を発生し、今までの識別符号codeｒに連接する。小さくない場合には、ステップＳ８０で、識別符号codeｒの１ビットｂ$^{(j)}$ を発生し、今までの識別符号に連接する。

【０１１８】この後、ステップＳ８２で変数ｊがｐ以上か否かを判定する。ノーの場合は、ステップＳ８４で変数ｊをインクリメント（＋１）して、ステップＳ７２に戻り、変数ｊがｉmod ｐに等しいか否かを判定する。ステップＳ８２でイエスの判定が得られた場合は、識別符

号code$_r$の全ビット（ｐビット）の発生、連接が終了したとして、code$_s$の発生に移る。

【０１１９】ステップＳ８６で、変数ｊに１をセットし、code$_s$に初期値（ビット長：０）をセットする。ステップＳ８８で、変数ｊがｉmod ｑと等しいか否かを判定する。等しい場合は、ステップＳ９０で識別符号code$_s$の１ビット$a^{(j)}$を発生し、今までの識別符号code$_s$に連接する。等しくない場合には、ステップＳ９２で変数ｊがｉmod ｑより小さいか否かを判定する。小さい場合は、ステップＳ９４で識別符号code$_s$の１ビット$c^{(j)}$を発生し、今までの識別符号code$_s$に連接する。小さくない場合には、ステップＳ９６で、識別符号code$_s$の１ビット$b^{(j)}$を発生し、今までの識別符号に連接する。

【０１２０】この後、ステップＳ９８で変数ｊがｑ以上か否かを判定する。ノーの場合は、ステップＳ１００で変数ｊをインクリメント（＋１）して、ステップＳ８８に戻り、変数ｊがｉmod ｑに等しいか否かを判定する。ステップＳ９８でイエスの判定が得られた場合は、識別符号code$_s$の全ビット（ｑビット）の発生、連接が終了したとして、ステップＳ１０２でcode$_r$とcode$_s$とを連接し、識別符号の発生を終了する。

【０１２１】このように識別符号を２つの部分に分けたことにより、符号量はＮのオーダではなく、（ｐのオーダ）＋（ｑのオーダ）となる。ここで、$p \fallingdotseq q$とすると、$p^2 \fallingdotseq q^2 \fallingdotseq N$となり、識別符号の長さは$N^{1/2}$のオーダとなる。

【０１２２】なお、第４実施形態においては、ｒとしてはｒ１とｒ２が求められ、ｓとしてはｓ１とｓ２が求められるので、結託者はｒ１とｓ１とで決まる１名とｒ２とｓ２とで決まる１名か、あるいはｒ１とｓ２とで決まる１名とｒ２とｓ１とで決まる１名であるのか特定できない。そこで、この一方を特定するためには、さらに次のような第３の整数ｔを導入する必要がある。ｎmod ｔ＝ｕとする。

【０１２３】$N=p\times q$、
$N \leqq p\times t$、
$N \leqq q\times t$
これから、ｒとしてはｒ１とｒ２が求められ、ｓとしてはｓ１とｓ２が求められ、ｔとしてはｔ１とｔ２が求められる。ｒとｓから結託者はｒ１とｓ１とで決まる１名とｒ２とｓ２とで決まる１名である（これをｎ１、ｎ２とする）か、あるいはｒ１とｓ２で決まる１名とｒ２とｓ１とで決まる１名である（これをｎ１’、ｎ２’とする）ことが分かる。ｓとｔから結託者はｓ１とｔ１とで決まる１名とｓ２とｔ２とで決まる１名である（これをｍ１、ｍ２とする）か、あるいはｓ$_1$とｔ$_2$で決まる１名とｓ$_2$とｔ$_1$とで決まる１名である（これをｍ１’、ｍ２’とする）ことが分かる。これら４通りの候補：（ｎ１、ｎ２）、（ｎ１’、ｎ２’）、（ｍ１、ｍ２）、（ｍ１’、ｍ２’）の中から一致するものが結託者であると判定する。

【０１２４】第４実施形態の識別符号復号器４８のアルゴリズムは、図１２に示した第３実施形態のアルゴリズムを整数ｐ、ｑに対してそれぞれ実行すればよい。このアルゴリズムを図１５、図１６に示す。ステップＳ２７２で、識別対象（ユーザ）ｕ１、ｕ２、…ｕ$_N$に埋め込み時と同じ順序を与える（$u_1<u_2<\cdots<u_{max}$）とともに、埋め込み時と同じ整数ｐ、ｑを与える。ステップＳ２７４で、変数ｉに１をセットし、codeの初期値として入力された抽出符号をセットし、第１の結託者の候補であるcandidate －ｐ１に１をセットし、第２の結託者の候補であるcandidate －ｐ２に１をセットする。ステップＳ２７６で、codeの先頭の符号が$c^{(i)}$であるか否かを判定する。イエスの場合は、ステップＳ２７８で変数ｉをインクリメント（＋１）し、ステップＳ２８０で第１の結託者の候補であるcandidate －ｐ１、及び第２の結託者の候補であるcandidate －ｐ２をそれぞれインクリメント（＋１）する。ステップＳ２８２でcodeを$c^{(i)}$の長さだけ左へシフトし、ステップＳ２７６のcodeの先頭の符号の判定に戻る。ステップＳ２７６でノーの判定が得られた場合は、ステップＳ２８４で変数ｉをインクリメント（＋１）し、codeを$c^{(i)}$の長さだけ左へシフトし、ステップＳ２８６で、codeの先頭の符号が$b^{(i)}$であるか否かを判定する。ノーの場合は、ステップＳ２８８で第２の結託者の候補であるcandidate －ｐ２にｉをセットし、ステップＳ２８４へ戻る。ステップＳ２８６でイエスの判定が得られた場合は、ステップＳ２９０で、変数ｉがｐ以上であるか否か判定する。

【０１２５】ノーの場合は、ステップＳ２８４に戻り、イエスの場合は、ステップＳ２９２で、第１の結託者の候補であるcandidate －ｑ１に１をセットし、第２の結託者の候補であるcandidate －ｑ２に１をセットする。ステップＳ２９４で、変数ｉをインクリメント（＋１）し、ステップＳ２９６で、codeの先頭の符号が$c^{(i)}$であるか否かを判定する。イエスの場合は、ステップＳ２９８で、変数ｉをインクリメント（＋１）し、ステップＳ３００で第１の結託者の候補であるcandidate －ｑ１、及び第２の結託者の候補であるcandidate －ｑ２をそれぞれインクリメント（＋１）する。ステップＳ３０２でcodeを$c^{(i)}$の長さだけ左へシフトし、ステップＳ２９６のcodeの先頭の符号の判定に戻る。ステップＳ２９６でノーの判定が得られた場合は、ステップＳ３０４で変数ｉをインクリメント（＋１）し、codeを$c^{(i)}$の長さだけ左へシフトし、ステップＳ３０６で、codeの先頭の符号が$b^{(i)}$であるか否かを判定する。ノーの場合は、ステップＳ３０８で第２の結託者の候補であるcandidate －ｑ２にｉをセットし、ステップＳ３０４へ戻る。ステップＳ３０６でイエスの判定が得られた場合は、ステップＳ３１０で、変数ｉがｐ＋ｑ以上であるか

否か判定する。ノーの場合は、ステップＳ３０４に戻り、イエスの場合は、ステップＳ３１２で、（candidate －ｐ１，candidate－ｑ１），（candidate －ｐ２，candidate －ｑ２），（candidate －ｐ１，candidate －ｑ２），（candidate －ｐ２，candidate －ｑ１）に対して中国人剰余定理を適用し、結託ユーザの候補の順位ｎを計算し、決定する。

【０１２６】上述した第４実施形態は、２つの整数ｐ、ｑの組み合わせを用いたが、中国人剰余定理の通り、ｋ個の整数ｐ１、ｐ２、…ｐｋを用いることもできる。この場合、ｖｉ＝Ｎmod ｐｉとし、ｖｉからｎを求めるアルゴリズムを図１７に示す。

【０１２７】ステップＳ１２０で変数ｉに１をセットする。ステップＳ１２２でｙｉ＝ｉｎｖ（（Ｎ／ｐｉ）mod ｐｉ，ｐｉ）を求める。ステップＳ１２４で変数ｉがｋ以上であるか否か判定する。ノーの場合は、ステップＳ１２６で変数ｉをインクリメント（＋１）し、ステップＳ１２２を再度実行する。ステップＳ１２４でイエスの判定が得られたら、ステップＳ１２８でｘに初期値０をセットし、ステップＳ１３０で変数ｉに再度０をセットする。ステップＳ１３２でｘ＝ｘ（ｘ＋（Ｎ／ｐｉ）・ｙｉ・ｖｉ）mod Ｎを計算する。ステップＳ１３４で変数ｉがｋ以上であるか否か判定する。ノーの場合は、ステップＳ１３６で変数ｉをインクリメント（＋１）し、ステップＳ１３２を再度実行する。ステップＳ１３４でイエスの判定が得られたら、ステップＳ１３８でｘをユーザｎを特定する情報として出力する。

【０１２８】本発明は上述した実施形態に限定されず、種々変形して実施可能である。例えば、上記実施形態は、ディジタルデータを配布する提供者側で識別符号を生成するとともに、ディジタルデータに埋め込んだが、識別符号の生成と、埋め込みとを分離してもよい。すなわち、識別符号は、信頼できる第３者が行い、生成した識別符号をクライアントであるディジタルデータ提供者に配布し、提供者側では、配布された識別符号をそのまま埋め込む。

【０１２９】このようにすると、識別符号を電子透かし以外の目的で利用できる。例えば、ユーザにその存在が知覚できるが、その符号の意味を教えていない形で、メッセージの一部として授受することができる。また、ユーザ名の識別以外の目的にも利用できる。利用の日付、日時、利用者端末の識別、ディジタルデータの識別、ディジタルデータの転送経路の識別、利用の条件の記述等としても利用できる。

【０１３０】

【発明の効果】以上説明したように本発明によれば、ディジタルデータに、そのデータのユーザ等に関する透かしデータを埋め込み、隠し持たせる電子透かし埋め込み装置において、複数のユーザが結託して互いのデータを比較したとしても、透かしデータを他のユーザに関する透かしデータに改竄することが困難とすることができる。

【図面の簡単な説明】

【図１】本発明による電子透かし埋め込み装置の第１の実施形態の構成を示すブロック図。

【図２】第１の実施形態の変形例の構成を示すブロック図。

【図３】図１中のデータ変換割当て部の詳細な構成を示すブロック図。

【図４】図１中のデータ変換割当て部の変形例のブロック図。

【図５】第１実施形態における識別符号の発生アルゴリズムを示すフローチャート。

【図６】第１実施形態における透かし検出装置の構成を示すブロック図。

【図７】第１実施形態の変形例における透かし検出装置の構成を示すブロック図。

【図８】第１実施形態における識別符号の復号のアルゴリズムを示すフローチャート。

【図９】本発明の第２実施形態における識別符号の発生アルゴリズムを示すフローチャート。

【図１０】第２実施形態における識別符号の復号のアルゴリズムを示すフローチャート。

【図１１】本発明の第３実施形態における識別符号の発生アルゴリズムを示すフローチャート。

【図１２】第３実施形態における識別符号の復号のアルゴリズムを示すフローチャート。

【図１３】本発明の第４実施形態における識別符号の発生アルゴリズムの前半を示すフローチャート。

【図１４】本発明の第４実施形態における識別符号の発生アルゴリズムの後半を示すフローチャート。

【図１５】本発明の第４実施形態における識別符号の復号のアルゴリズムの前半を示すフローチャート。

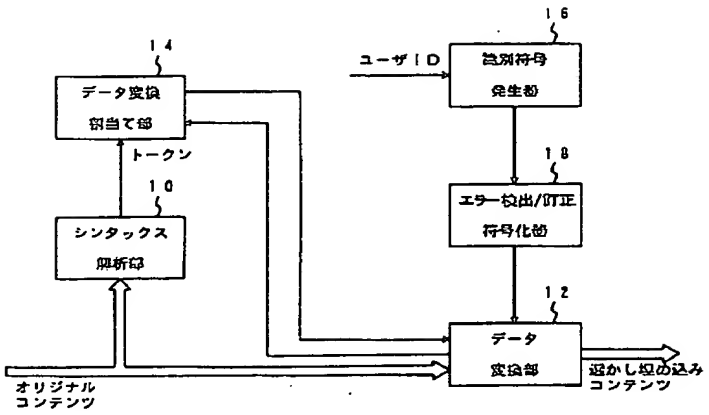
【図１６】本発明の第４実施形態における識別符号の復号のアルゴリズムの後半を示すフローチャート。

【図１７】本発明の第４実施形態の変形例における識別符号の発生アルゴリズムを示すフローチャート。

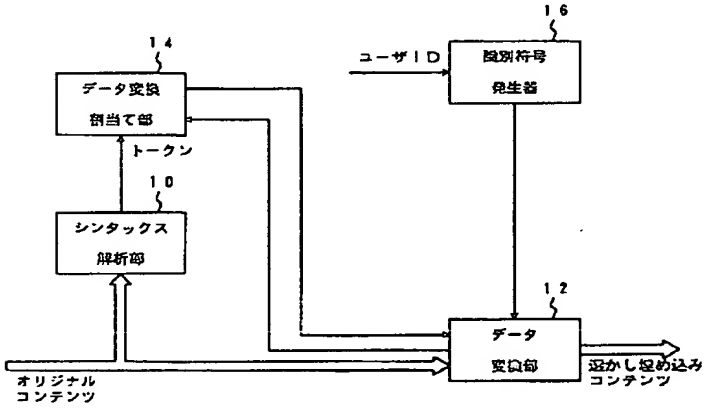
【符号の説明】

１０…シンタックス解析部
１２…データ変換部
１４…データ変換割当て部
１６…識別符号発生器
１８…エラー検出／訂正符号化器

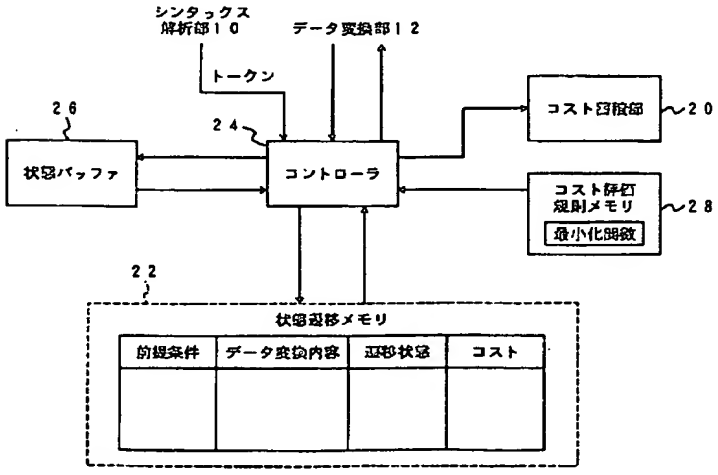
【図１】


16
ユーザＩＤ
識別符号
発生器
14
データ変換
割当て部
トークン
18
エラー検出/訂正
符号化器
10
シンタックス
解析部
12
データ
変換部
オリジナル
コンテンツ
透かし埋め込み
コンテンツ

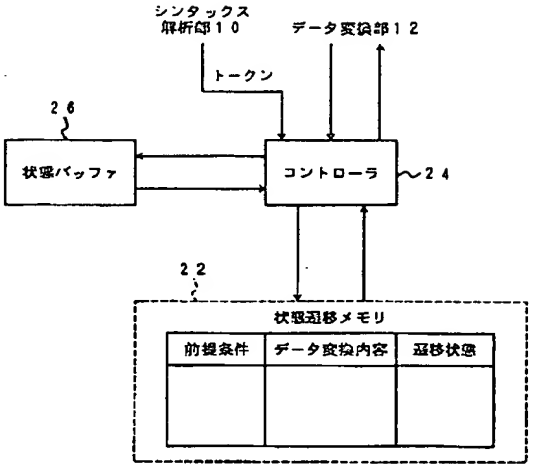
【図２】


16
ユーザＩＤ
識別符号
発生器
14
データ変換
割当て部
トークン
10
シンタックス
解析部
12
データ
変換部
オリジナル
コンテンツ
透かし埋め込み
コンテンツ

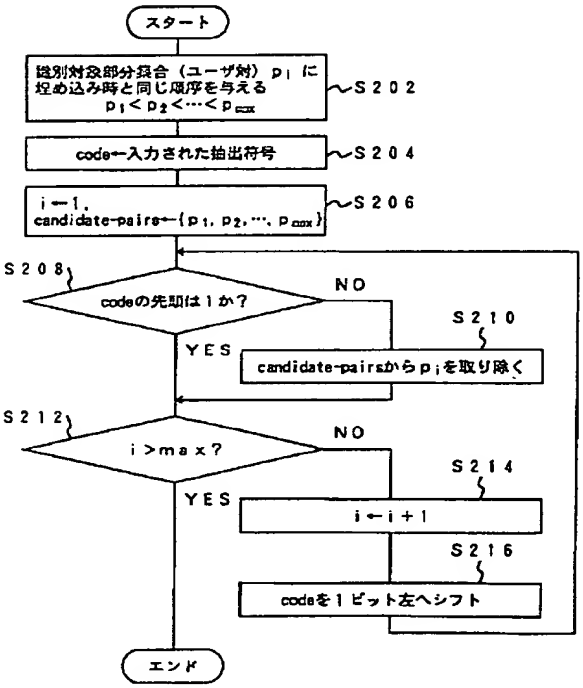
【図３】


シンタックス
解析部１０
データ変換部１２
トークン
２６
２４
状態バッファ
コントローラ
コスト関数部
２０
コスト評価
規則メモリ
２８
最小化関数
２２
状態遷移メモリ
前提条件
データ変換内容
遷移状態
コスト

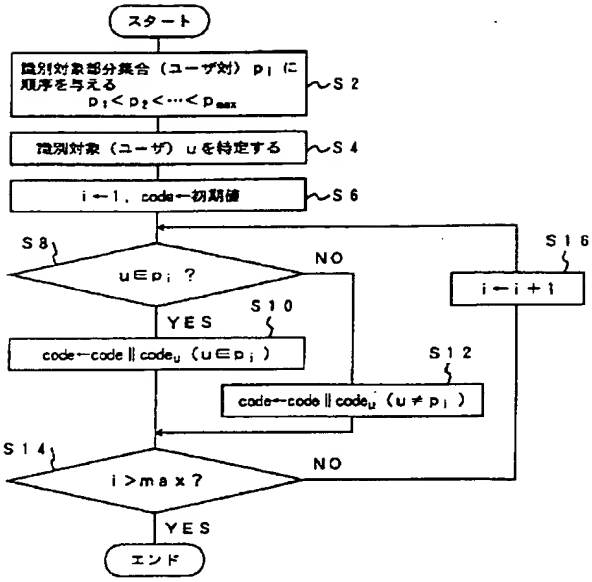
【図４】


シンタックス
解析部１０
データ変換部１２
トークン
２６
状態バッファ
コントローラ
２４
２２
状態遷移メモリ
前提条件
データ変換内容
遷移状態

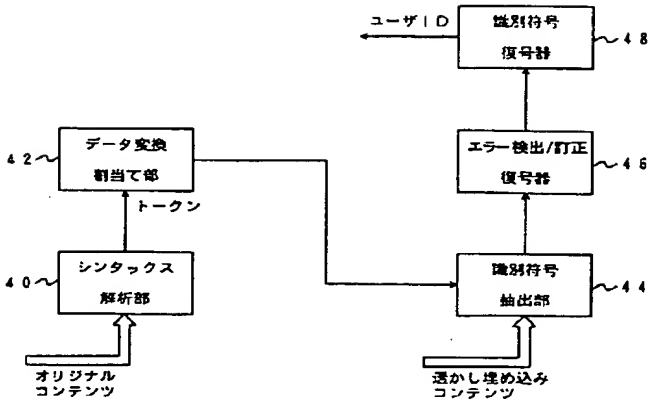
【図８】


スタート
識別対象部分集合（ユーザ対）p_i に
埋め込み時と同じ順序を与える
$p_1 < p_2 < \cdots < p_{max}$
S２０２
code←入力された抽出符号
S２０４
i←1,
candidate-pairs←{$p_1, p_2, \cdots, p_{max}$}
S２０６
S２０８
codeの先頭は１か？
NO
YES
S２１０
candidate-pairsからp_iを取り除く
S２１２
i＞max？
NO
YES
S２１４
i←i＋１
S２１６
codeを１ビット左へシフト
エンド

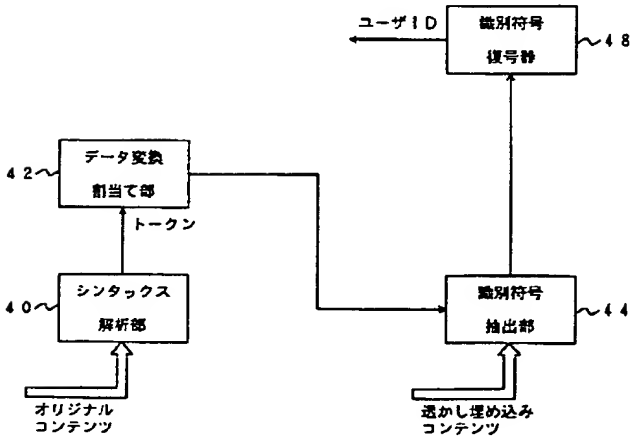
【図５】


スタート
識別対象部分集合（ユーザ対）p_i に順序を与える
$p_1 < p_2 < \cdots < p_{max}$
S２
識別対象（ユーザ）uを特定する
S４
i←1，code←初期値
S６
S８
$u \in p_i$ ？
NO
YES
S１０
$code \leftarrow code \| code_u$ $(u \in p_i)$
S１２
$code \leftarrow code \| code_u$ $(u \neq p_i)$
S１６
i←i＋1
S１４
i＞max？
NO
YES
エンド

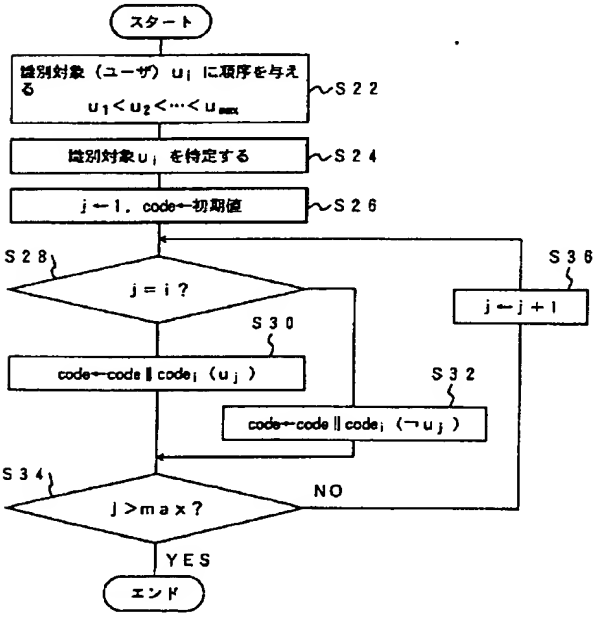
【図６】


ユーザＩＤ
識別符号復号器
４８
データ変換前当て部
４２
トークン
シンタックス解析部
４０
エラー検出/訂正復号器
４６
識別符号抽出部
４４
オリジナルコンテンツ
透かし埋め込みコンテンツ

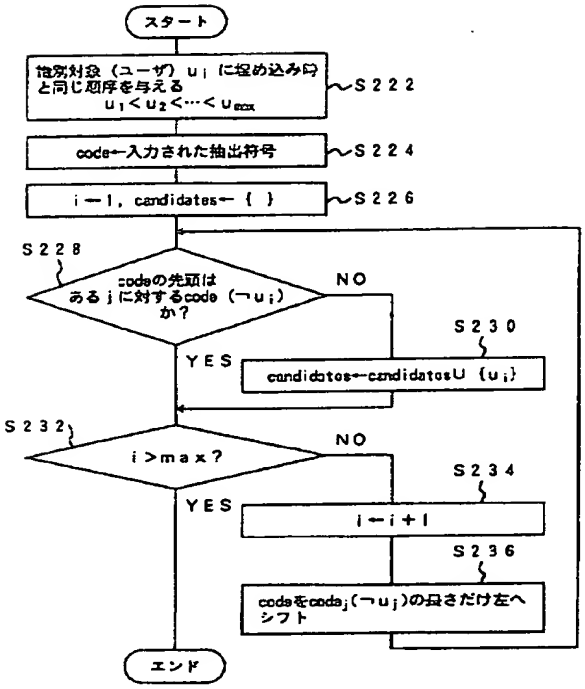
【図７】


ユーザＩＤ
識別符号復号器
４８
データ変換前当て部
４２
トークン
シンタックス解析部
４０
識別符号抽出部
４４
オリジナルコンテンツ
透かし埋め込みコンテンツ

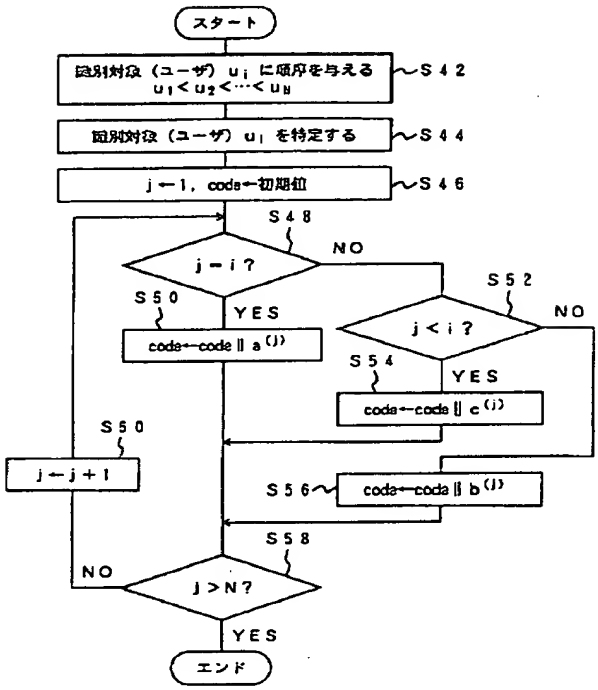
【図９】


スタート
識別対象（ユーザ）u_i に順序を与える
$u_1 < u_2 < \cdots < u_{max}$
S２２
識別対象u_iを特定する
S２４
j←1，code←初期値
S２６
S２８
j＝i？
S３０
$code \leftarrow code \| code_i$ (u_j)
S３２
$code \leftarrow code \| code_i$ $(\neg u_j)$
S３６
j←j＋1
S３４
j＞max？
NO
YES
エンド

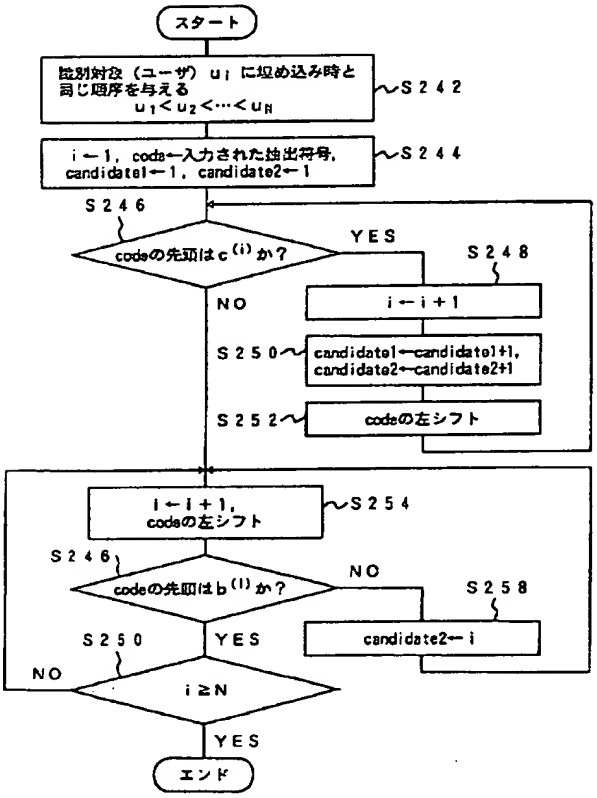
【図１０】



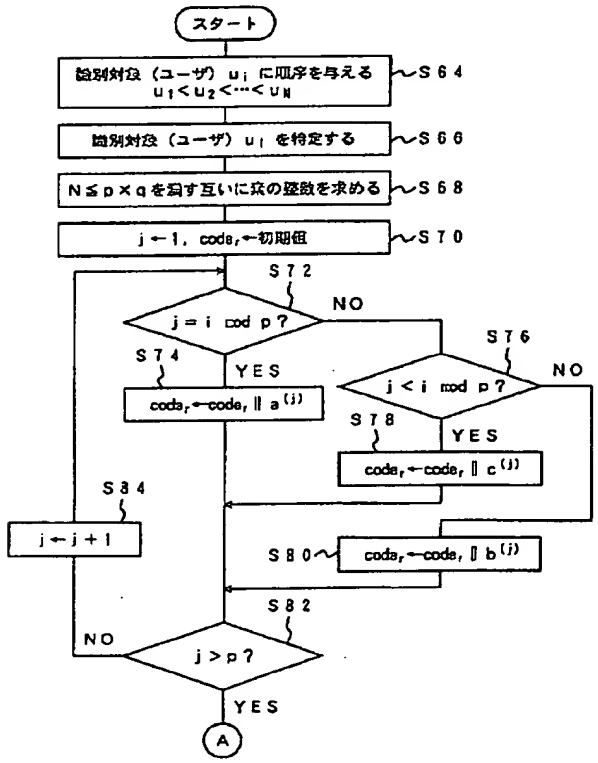
【図１１】



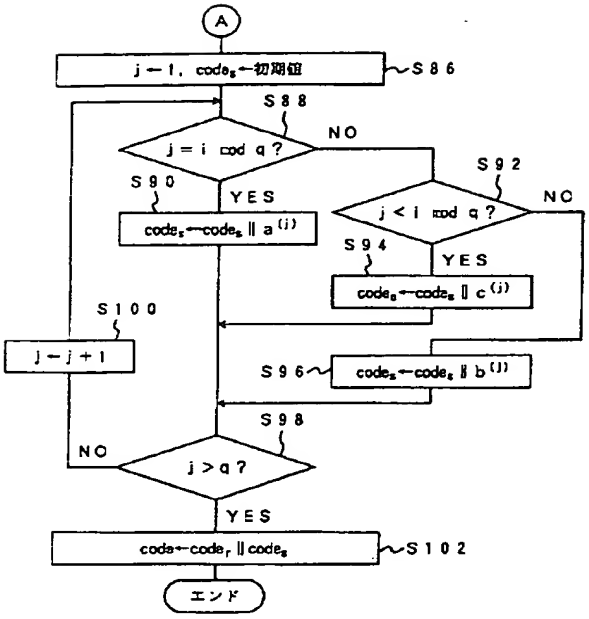
【図１２】



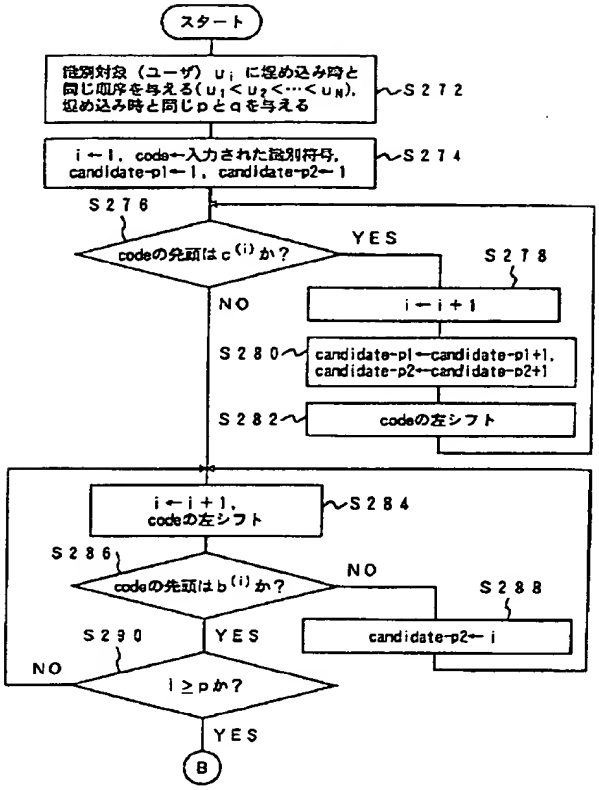
【図１３】



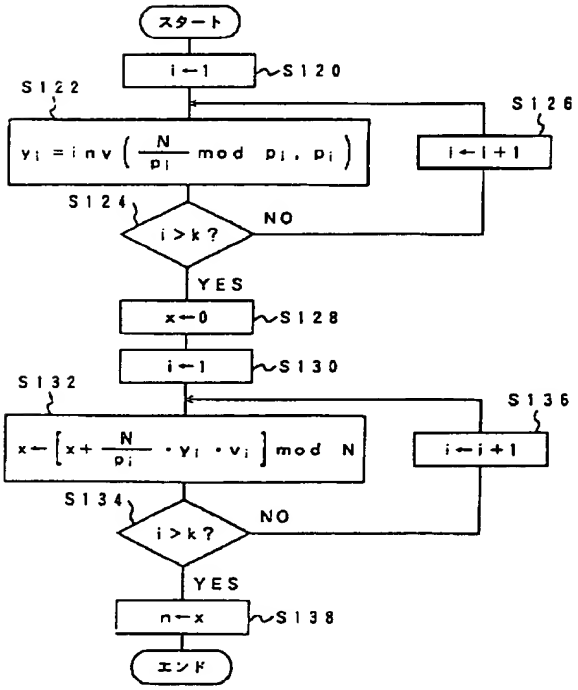
【図１４】


A
j←1, code_s←初期値
S86
S88
j = i mod q ?
NO
YES
S90
code_s←code_s ‖ a^(i)
S92
j < i mod q ?
NO
YES
S94
code_s←code_s ‖ c^(j)
S100
j←j+1
S96
code_s←code_s ‖ b^(j)
S98
j > q ?
NO
YES
coda←code_r ‖ code_s
S102
エンド

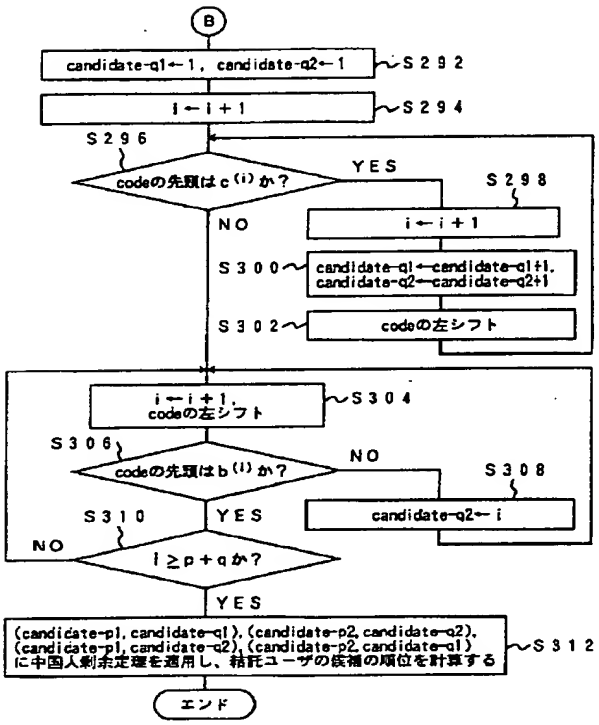
【図１５】


スタート
識別対象（ユーザ）u_i に埋め込み時と同じ順序を与える（u_1 < u_2 <…< u_N）．埋め込み時と同じｐとｑを与える
S272
i←1，code←入力された識別符号，candidate-p1←1，candidate-p2←1
S274
S276
codeの先頭は c^(i) か？
YES
S278
i←i+1
NO
S280
candidate-p1←candidate-p1+1，candidate-p2←candidate-p2+1
S282
codeの左シフト
i←i+1，codeの左シフト
S284
S286
codeの先頭は b^(i) か？
NO
S288
candidate-p2←i
S290
YES
NO
i ≥ p か？
YES
B

【図１７】


スタート
i←1
S120
S122
y_i = inv(N/p_i mod p_i , p_i)
S126
i←i+1
S124
i > k ?
NO
YES
x←0
S128
i←1
S130
S132
x←[x + N/p_i · y_i · v_i] mod N
S136
i←i+1
S134
i > k ?
NO
YES
n←x
S138
エンド

【図１６】



【手続補正書】
【提出日】平成１１年５月１７日（１９９９．５．１７）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、
ユーザを識別する情報として、ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする電子透かし埋め込み装置。
【請求項２】　ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、
ユーザを識別する情報として、当該ユーザがディジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を論理積の形で連接して用いることを特徴とする電子透かし埋め込み装置。
【請求項３】　ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、
ユーザを識別する情報として、ディジタルデータを渡す可能性のあるユーザの各々に順位を付け、当該ユーザが各ユーザより順位が小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接して用いることを特徴とする電子透かし埋め込み装置。
【請求項４】　ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、
ユーザを識別する情報として、ディジタルデータを渡す可能性のあるユーザの各々に順位を付け、ディジタルデータを渡す可能性のあるユーザの総数をＮとし、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑそれぞれに対して、ｐを法とした当該ユーザの順位ｎの剰余が０からｐ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報と、ｑを法とした当該ユーザの順位ｎの剰余が０からｑ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報とをユ

ーザを識別する情報として用いることを特徴とする電子透かし埋め込み装置。

【請求項５】 ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、全対象物の中の任意の２つの対象物の対の各々に対して、当該対象物がその対に含まれているか否かを表わす情報を発生することを特徴とする識別情報発生装置。

【請求項６】 ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、当該対象物が全対象物の中の各対象物であるか否かを表わす情報を論理積の形で連接した情報を発生することを特徴とする識別情報発生装置。

【請求項７】 ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、全識別対象物の各々に順位を付け、当該対象物が各識別対象物より順位が小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報を発生することを特徴とする識別情報発生装置。

【請求項８】 全識別対象物の総数をＮとし、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑそれぞれに対して、ｐを法とした当該対象物の順位ｎの剰余が０からｐ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報と、ｑを法とした当該対象物の順位ｎの剰余が０からｑ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報とを識別情報として発生することを特徴とする請求項７に記載の識別情報発生装置。

【請求項９】 ディジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、

種々のデータ変換内容を記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、

請求項５乃至請求項８のいずれか１項に記載の識別情報発生装置と、

前記データ割当て部から出力されたデータ変換内容と前記識別情報発生装置から出力された識別情報に応じて、ディジタルデータの所定の部分を変更する識別情報埋め込み手段と、

を具備することを特徴とする識別情報埋め込み装置。

【請求項１０】 ディジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、

種々のデータ変換内容をその変化程度を表わすコストと共に記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、

データ変換後のデータの変化程度を累積する手段と、

請求項５乃至請求項８のいずれか１項に記載の識別情報発生装置と、

前記データ割当て部から出力されたデータ変換内容と前記識別情報発生装置から出力された識別情報に応じて、ディジタルデータの所定の部分を変更する識別情報埋め込み手段と、

前記累積手段により、データの変化程度の累積値が所定の変化程度を超える場合、前記識別情報埋め込み手段の動作を禁止する手段とを具備することを特徴とする識別情報埋め込み装置。

【請求項１１】 請求項１乃至請求項４のいずれか１項に記載の電子透かし埋め込み装置により、ユーザを識別する情報がユーザには知覚できないように符号化されて埋め込まれているディジタルデータから識別情報を読み取る識別情報検出装置において、

ディジタルデータの所定の位置に埋め込まれている識別符号を抽出する手段と、

抽出された識別符号を復号し、識別情報を求める手段と、

を具備することを特徴とする識別情報検出装置。

【請求項１２】 請求項１に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、

ディジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、

その部位が請求項１に記載の装置により埋め込まれた、そのユーザ対がこのディジタルデータに対応するユーザを含んでいることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、

その部位が請求項１に記載の装置により埋め込まれた、そのユーザ対がこのディジタルデータに対応するユーザを含んでいることを表わす符号であると判定されたユーザ対を結託したユーザ対の候補と推定することを特徴とする識別情報読取方法。

【請求項１３】 請求項２に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、

ディジタルデータから抽出された識別情報から各ユーザに対応する部位を読み取るステップと、

その部位が請求項２に記載の装置により埋め込まれた、そのユーザがこのディジタルデータに対応するユーザであることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、

その部位が請求項２に記載の装置により埋め込まれた、そのユーザがこのディジタルデータに対応するユーザであることを表わす符号であると判定されたユーザを結託したユーザの候補と推定することを特徴とする識別情報読取方法。

【請求項１４】請求項３に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、

１）ディジタルデータから抽出された識別情報から各ユーザに対応する部位を順次読み取るステップと、
２）その部位が請求項３に記載の装置により埋め込まれた、そのユーザの順位がこのディジタルデータに対応するユーザの順位よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ１）、２）を繰り返すステップと、
３）上記ステップ２）において、初めて現れたそれ以外の符号の次の部位から、各ユーザに対応する部位を順次読み取るステップと、
４）その部位が請求項３に記載の装置により埋め込まれた、そのユーザの順位がこのディジタルデータに対応するユーザの順位よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ３）、４）を繰り返すステップと、
５）抽出された識別情報の最後に到達するまで上記ステップ３）、４）、５）を繰り返すステップと、を具備し、
上記ステップ２）において、それ以外の符号が初めて現れた部位に対応するユーザを第一の結託ユーザ候補と推定し、
上記ステップ４）において、それ以外の符号が最後に現れた部位に対応するユーザを第二の結託ユーザ候補と推定することを特徴とする識別情報読取方法。
【請求項１５】　請求項４に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、
１）ディジタルデータから抽出された識別情報からｐを法とするユーザのそれぞれに対応する部位を順次読み取るステップと、
２）その部位が、請求項４に記載の装置により埋め込まれた、ｐを法としたそのユーザの順位の剰余がｐを法としたこのディジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ１）、２）を繰り返すステップと、
３）上記ステップ２）において、初めて現れたそれ以外の符号を次の部位から、ｐを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
４）その部位が、請求項４に記載の装置により埋め込まれた、ｐを法としたそのユーザ順位の剰余がｐを法としたこのディジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ３）、４）を繰り返すステップと、
５）抽出された識別情報からｐを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ３）、４）、５）を繰り返すステップと、
６）上記ステップ５）において、抽出された識別情報からｐを法としたユーザ順位の剰余のすべての部位を読み取った後、その次の部位からｑを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
７）その部位が、請求項４に記載の装置により埋め込まれた、ｑを法としたそのユーザの順位の剰余がｑを法としたこのディジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ６）、７）を繰り返すステップと、
８）上記ステップ７）において、初めて現れたそれ以外の符号を次の部位から、ｑを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
９）その部位が、請求項４に記載の装置により埋め込まれた、ｑを法としたそのユーザ順位の剰余がｑを法としたこのディジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ８）、９）を繰り返すステップと、
１０）抽出された識別情報からｑを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ８）、９）、１０）を繰り返すステップと、を具備し、上記ステップ２）において、それ以外の符号が初めて現れた部位に対応するｐを法としたユーザ順位の剰余と、上記ステップ４）において、それ以外の符号が最後に現れた部位に対応するｐを法としたユーザ順位の剰余と、上記ステップ７）において、それ以外の符号が初めて現れた部位に対応するｑを法としたユーザ順位の剰余と、上記ステップ９）において、それ以外の符号が最後に現れた部位に対応するｑを法としたユーザ順位の剰余とを組み合わせて構成されるｐを法とする剰余とｑを法とする剰余の組に対して中国人剰余定理を適用して結託ユーザの候補を推定することを特徴とする識別情報読取方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正内容】
【００１７】
【発明が解決しようとする課題】このように従来の電子透かし埋め込み技術は、ユーザを識別する透かしデータを当該ユーザには知覚できない状態で埋め込み、隠し持たせることができるが、複数のユーザが結託してデータを互いに比較することにより、透かしデータが埋め込まれている位置に関する情報を得ることができてしまい、透かしデータの偽造や消去を容易にするという欠点があった。また、結託したユーザを特定できるような識別情報の埋め込み法もあるが、結託に参加したユーザが２人の場合しか特定できず、３人以上のユーザが結託した場

合は、特定できない欠点がある。また、必ずしも結託ユーザを特定できない場合もあり、結託ユーザを特定できる確率が低かった。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正内容】
【００１８】本発明の目的は、複数のユーザが結託して互いのデータを比較したとしても、埋め込まれている透かしデータに関する情報を十分に得ることができず、透かしデータを偽造や消去することが困難となるように、ディジタルデータに、そのデータのユーザ等に関する透かしデータを埋め込み、隠し持たせることができ、しかも３人以上のユーザが結託して透かしデータを改竄した場合でも、高い確率で結託したユーザを特定できる電子透かし埋め込み装置を提供することである。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正内容】
【００２０】（１）ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、ディジタルデータを渡す可能性のある全ユーザの中の任意の２人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正内容】
【００２１】（２）ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、当該ユーザがディジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を論理積の形で連接して用いることを特徴とする。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】変更
【補正内容】
【００２２】（３）ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、ディジタルデータを渡す可能性のあるユーザの各々に順位を付け、当該ユーザが各ユーザより順位が小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接して用いることを特徴とする。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更
【補正内容】
【００２３】（４）ユーザに渡すディジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、ディジタルデータを渡す可能性のあるユーザの各々に順位を付け、ディジタルデータを渡す可能性のあるユーザの総数をＮとし、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑそれぞれに対して、ｐを法とした当該ユーザの順位ｎの剰余が０からｐ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報と、ｑを法とした当該ユーザの順位ｎの剰余が０からｑ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報とをユーザを識別する情報として用いることを特徴とする。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】変更
【補正内容】
【００２４】（５）ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、全対象物の中の任意の２つの対象物の対の各々に対して、当該対象物がその対に含まれているか否かを表わす情報を発生することを特徴とする。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】変更
【補正内容】
【００２５】（６）ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、当該対象物が全対象物の中の各対象物であるか否かを表わす情報を論理積の形で連接した情報を発生することを特徴とする。

【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】変更
【補正内容】
【００２６】（７）ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、全識別対象物の各々に順位を付け、当該対象物が各識別対

象物より順位が小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報を発生することを特徴とする。

【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】変更
【補正内容】
【００２７】（８）全識別対象物の総数をＮとし、Ｎ≦ｐ×ｑとなる互いに素の整数ｐ、ｑそれぞれに対して、ｐを法とした当該対象物の順位ｎの剰余が０からｐ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報と、ｑを法とした当該対象物の順位ｎの剰余が０からｑ－１までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で連接した情報とを識別情報として発生することを特徴とする。

【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】変更
【補正内容】
【００２８】（９）ディジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容を記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、（５）乃至（８）のいずれかに記載の識別情報発生装置と、前記データ割当て部から出力されたデータ変換内容と前記識別情報発生装置から出力された識別情報に応じて、ディジタルデータの所定の部分を変更する識別情報埋め込み手段と、を具備することを特徴とする識別情報埋め込み装置。

【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】変更
【補正内容】
【００２９】（１０）ディジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容をその変化程度を表わすコストと共に記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、データ変換後のデータの変化程度を累積する手段と、（５）乃至（８）のいずれかに記載の識別情報発生装置と、前記データ割当て部から出力されたデータ変換内容と前記識別情報発生装置から出力された識別情報に応じて、ディジタルデータの所定の部分を変更する識別情報埋め込み手段と、前記累積手段により、データの変化程度の累積値が所定の変化程度を超える場合、前記識別情報埋め込み手段の動作を禁止する手段とを具備することを特徴とする識別情報埋め込み装置。

【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００３０
【補正方法】変更
【補正内容】
【００３０】（１１）　（１）乃至（４）のいずれかに記載の電子透かし埋め込み装置により、ユーザを識別する情報がユーザには知覚できないように符号化されて埋め込まれているディジタルデータから識別情報を読み取る識別情報検出装置において、ディジタルデータの所定の位置に埋め込まれている識別符号を抽出する手段と、抽出された識別符号を復号し、識別情報を求める手段と、を具備することを特徴とする。

【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】変更
【補正内容】
【００３１】（１２）　（１）に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、ディジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、その部位が（１）に記載の装置により埋め込まれた、そのユーザ対がこのディジタルデータに対応するユーザを含んでいることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が（１）に記載の装置により埋め込まれた、そのユーザ対がこのディジタルデータに対応するユーザを含んでいることを表わす符号であると判定されたユーザ対を結託したユーザ対の候補と推定することを特徴とする。

【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００３２
【補正方法】変更
【補正内容】
【００３２】（１３）　（２）に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、ディジタルデータから抽出された識別情報から各ユーザに対応する部位を読み取るステップと、その部位が（２）に記載の装置により埋め込まれた、そのユーザがこのディジタルデータに対応するユーザであることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が（２）に記載の装置により埋め込まれた、そのユーザがこのディジタルデータに対応するユーザであることを表わす符号であると判定

されたユーザを結託したユーザの候補と推定することを特徴とする。

【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】００３３
【補正方法】変更
【補正内容】
【００３３】（１４）　（３）に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、
１）ディジタルデータから抽出された識別情報から各ユーザに対応する部位を順次読み取るステップと、
２）その部位が請求項３に記載の装置により埋め込まれた、そのユーザの順位がこのディジタルデータに対応するユーザの順位よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ１）、２）を繰り返すステップと、
３）上記ステップ２）において、初めて現れたそれ以外の符号の次の部位から、各ユーザに対応する部位を順次読み取るステップと、
４）その部位が（３）に記載の装置により埋め込まれた、そのユーザの順位がこのディジタルデータに対応するユーザの順位よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ３）、４）を繰り返すステップと、
５）抽出された識別情報の最後に到達するまで上記ステップ３）、４）、５）を繰り返すステップと、を具備し、上記ステップ２）において、それ以外の符号が初めて現れた部位に対応するユーザを第一の結託ユーザ候補と推定し、上記ステップ４）において、それ以外の符号が最後に現れた部位に対応するユーザを第二の結託ユーザ候補と推定することを特徴とする。

【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】変更
【補正内容】
【００３４】（１５）　（４）に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたディジタルデータから識別情報を読み取る方法において、
１）ディジタルデータから抽出された識別情報からｐを法とするユーザのそれぞれに対応する部位を順次読み取るステップと、
２）その部位が、（４）に記載の装置により埋め込まれた、ｐを法としたそのユーザの順位の剰余がｐを法としたこのディジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ１）、２）を繰り返すステップと、
３）上記ステップ２）において、初めて現れたそれ以外の符号を次の部位から、ｐを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
４）その部位が、（４）に記載の装置により埋め込まれた、ｐを法としたそのユーザ順位の剰余がｐを法としたこのディジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ３）、４）を繰り返すステップと、
５）抽出された識別情報からｐを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ３）、４）、５）を繰り返すステップと、
６）上記ステップ５）において、抽出された識別情報からｐを法としたユーザ順位の剰余のすべての部位を読み取った後、その次の部位からｑを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
７）その部位が、（４）に記載の装置により埋め込まれた、ｑを法としたそのユーザの順位の剰余がｑを法としたこのディジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ６）、７）を繰り返すステップと、
８）上記ステップ７）において、初めて現れたそれ以外の符号を次の部位から、ｑを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
９）その部位が、（４）に記載の装置により埋め込まれた、ｑを法としたそのユーザ順位の剰余がｑを法としたこのディジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ８）、９）を繰り返すステップと、
１０）抽出された識別情報からｑを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ８）、９）、１０）を繰り返すステップと、を具備し、上記ステップ２）において、それ以外の符号が初めて現れた部位に対応するｐを法としたユーザ順位の剰余と、上記ステップ４）において、それ以外の符号が最後に現れた部位に対応するｐを法としたユーザ順位の剰余と、上記ステップ７）において、それ以外の符号が初めて現れた部位に対応するｑを法としたユーザ順位の剰余と、上記ステップ９）において、それ以外の符号が最後に現れた部位に対応するｑを法としたユーザ順位の剰余とを組み合わせて構成されるｐを法とする剰余とｑを法とする剰余の組に対して中国人剰余定理を適用して結託ユーザの候補を推定することを特徴とする。

【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】００８６

【補正方法】変更
【補正内容】
【００８６】（第３実施形態）第２実施形態は上述の符号を用いる場合は、３人以上のユーザの結託には弱い。結託者が３人以上の場合には、例えば多数決攻撃（互いの差分のデータ“０”、“１”を多数のデータに書き換える）を行うことによって、どのユーザをも表さない連接された符号を偽造できる。しかし、ユーザａでないことをあらわす符号を複数用意することによって、多数決攻撃は有効でなくなる。なぜなら、ユーザａでないという符号が複数存在するので多数決によっては、ユーザａでないという符号を得ることができないからである。
【手続補正２０】
【補正対象書類名】明細書
【補正対象項目名】００８７
【補正方法】変更
【補正内容】
【００８７】上述のようにユーザａではないという符号を１個しか用いない場合の第２実施形態において、ユーザｕｉ、ｕｊ、ｕｋが結託する場合を考える。